NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FROM STICKS AND STONES TO ZEROS AND ONES: THE DEVELOPMENT OF COMPUTER NETWORK OPERATIONS AS AN ELEMENT OF WARFARE

A STUDY OF THE PALESTINIAN-ISRAELI CYBERCONFLICT AND WHAT THE UNITED STATES CAN LEARN FROM THE "INTERFADA"

by

Jacqueline-Marie Wilson Wrona

September 2005

Thesis Advisor:	Dan C. Boger
Second Reader:	Karl D. Pfeiffer

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE *Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE:
From Sticks and Stones to Zeros and Ones: The Development of Computer Network Operations as an Element of Warfare *A Study of the Palestinian-Israeli Cyberconflict and what the United States Can Learn from the "Interfada"*

5. FUNDING NUMBERS

6. AUTHOR(S) Jacqueline-Marie Wilson Wrona

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The Palestinian-Israeli Cyberconflict erupted in 2000, when Israeli hackers crippled the prime website of Hezbollah by mobilizing pro-Israeli supporters to "bomb" the site with automated floods of electronic mail. In retaliation, Hezbollah rallied pro-Arab supporters for a counter-attack, which soon downed the main Israeli government website and the Israeli Foreign Ministry site. Attacks involving website defacements, denial-of-service, viruses, and Trojan horses occurred by both parties for a span of months, effectively shutting down websites, disrupting Internet service and e-commerce.

A study and analysis of the utilization and effects of Computer Network Operations (CNO) between pro-Israeli and pro-Palestinian actors during the al-Aqsa Intifada may highlight current trends in warfare, support the notion that information may level the battlefield, and provide the United States with the means to better protect itself against such attacks in the future.

This thesis seeks to collect, classify, analyze, define, and resolve IO/IW; the utilization and effects of CNO during the Al-Aqsa Intifada, and how such analysis can be applied to United States national security.

14. SUBJECT TERMS
Information Warfare, Information Operations, Computer Network Operations, Palestinian-Israeli Cyberconflict, "Interfada"

15. NUMBER OF PAGES
151

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

FROM STICKS AND STONES TO ZEROS AND ONES: THE DEVELOPMENT OF COMPUTER NETWORK OPERATIONS AS AN ELEMENT OF WARFARE

A STUDY OF THE PALESTINIAN-ISRAELI CYBERCONFLICT AND WHAT THE UNITED STATES CAN LEARN FROM THE "INTERFADA"

Jacqueline-Marie Wilson Wrona
Ensign, United States Navy Reserve
B.S., United States Naval Academy, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY (COMMAND, CONTROL, AND COMMUNICATIONS (C3))

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Author: Jacqueline-Marie Wilson Wrona

Approved by: Dan C. Boger
Thesis Advisor

Karl D. Pfeiffer
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Palestinian-Israeli Cyberconflict erupted in 2000, when Israeli hackers crippled the prime website of Hezbollah by mobilizing pro-Israeli supporters to “bomb” the site with automated floods of electronic mail. In retaliation, Hezbollah rallied pro-Arab supporters for a counter-attack, which soon downed the main Israeli government website and the Israeli Foreign Ministry site. Attacks involving website defacements, denial-of-service, viruses, and Trojan horses occurred by both parties for a span of months, effectively shutting down websites, disrupting Internet service and e-commerce. As is evident by this turn of events, one need search no further than a computer savvy teenager and his laptop for an effective weapon of choice against an adversary’s economy, infrastructure, military, or government. Additionally, psychological operations, to include deception and propaganda, continue to influence one’s enemies, and at times the world audience, into acting in a manner conducive to one’s aims. In effect, the asymmetric element of information warfare may eventually level the battlefield between superpowers and minor states and/or terrorist organizations.

A study and analysis of the utilization and effects of Computer Network Operations (CNO) between pro-Israeli and pro-Palestinian actors during the al-Aqsa Intifada may highlight current trends in warfare, support the notion that information may level the battlefield, and provide the United States with the means to better protect itself against such attacks in the future.

This thesis seeks to collect, classify, analyze, define, and resolve Information Operations/Information Warfare (IO/IW) activities, specifically focused on the utilization and effects of CNO during the Al-Aqsa Intifada, and how such analysis can be applied to United States national security. Through analysis of the utilization and effects of IO/IW during the Al-Aqsa Intifada, the United States may be better able to prevent such attacks against its own networks and sources of information and infrastructure.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr. Dan C. Boger, Chairman of the Department of Information Sciences, and Lieutenant Colonel Karl D. Pfeiffer, USAF, Ph.D. for their guidance and assistance as Thesis Advisor and Second Reader, respectively. Their willingness to take a chance on an Ensign who wanted to do “outside” research allowed me the opportunity to research a region and conflict with which I am personally interested. Additionally, I would like to thank my mother, Patricia W. Wrona for her constant encouragement and support, proof-reading, and critique. Without my mother, I would not be the person I am today and would not have had the opportunity to pursue a Master of Science, let alone research and write a thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

This thesis will focus on Information Operations/Information Warfare (IO/IW), in particular the malicious use of the Internet and computer network operations during the al-Aqsa Intifada in Israel, through the analysis of primary and secondary resources.

While global defense establishments have yet to agree on the exact definition of the term "information warfare," everyone does agree that in the digital age, information and its dissemination have achieved the status of a vital strategic asset. Information technology is continuously being developed as both an offensive battlefield weapon, and as a means to disrupt the civilian infrastructure on which an enemy's government and, in turn, its military rely. The growing reliance upon technology has resulted in IW evolving into a double-edged sword: those most capable of waging IW become the ones most vulnerable to it.

The cyberattacks which began shortly after the uprisings resulting from Israeli Prime Minister Ariel Sharon's visit to the al-Aqsa mosque in Israel represent the first political conflict in which two sides have fought each other in an organized fashion via the Internet. Through the use of cyberattacks, both Palestinians and Israelis were able to infiltrate each other's websites, release viruses, and deny service to users via the information superhighway. Additionally, attacks against key government sites and infrastructure elevated the risks posed by such attacks.

In addition to cyberattacks, the media and military have been used to perform a number of information operations during the al-Aqsa Intifada. Through propaganda, news releases, and the use of unmanned aerial vehicles, just to mention a few methods, both the Israelis and Palestinians (along with their supporters) have waged successful information attacks against each other. This trend supports the notion that IO/IW may level the battlefield, and that such asymmetric methods used by weaker states and/or terrorist organizations may pose serious threats to world powers.

This thesis seeks to collect, classify, analyze, define, and resolve IO/IW; illustrate information-based methods utilized during the al-Aqsa Intifada, the effects of these methods, and how such analysis can be applied to United States national security. Through analysis of the utilization and effects of computer network operations during the al-Aqsa Intifada, the United States may be better able to prevent such attacks against its own networks and sources of information and infrastructure.

B. STATEMENT OF PROBLEM

The Arab-Israeli cyberwar first erupted in 2000, when Israeli hackers crippled the prime website of Hezbollah in Lebanon by mobilizing pro-Israeli supporters to “bomb” the site with automated floods of electronic mail. In retaliation, Hezbollah rallied pro-Arab supporters for a counter-attack which soon downed the main Israeli government website and the Israeli Foreign Ministry site. Daily attacks involving website defacements, denial of service, viruses, and Trojan horses occurred by both parties for a span of months, effectively shutting down websites. As is evident by this turn of events, one need search no further than a computer savvy teenager and his laptop for an effective weapon of choice against an adversary’s economy, infrastructure, military, or government. Additionally, psychological operations, to include deception and propaganda, continue to influence one’s enemies and, at times, the world audience, into acting in a manner conducive to one’s aims. In effect, the asymmetric element of information warfare may eventually level the battlefield between superpowers and minor states and/or terrorist organizations.

The increasing flow of information, the evolution of the global economy, and the creation of, and dependence on, the Internet are all contributing factors in the development of the modern global village. Like social trends, warfare is also shifting and the world will undoubtedly face its future conflicts not only on the battlefield, but in the realm of information. With increasing digitization of economies, infrastructure, battlefields, and governments; top officials are seeking out ways to protect the computerized control of one’s governmental and military apparatus, while at the same time developing means to disrupt that of the enemy. Unfortunately, the more technologically advanced a nation becomes, the more vulnerable it is to the techniques of information warfare.

A study and analysis of the utilization and effects of computer network operations between Israelis and Palestinians during the al-Aqsa Intifada may highlight current trends in warfare, support the notion that information may level the battlefield, and provide the United States with the means to better protect itself against such attacks in the future.

C. SCOPE OF THESIS

This thesis will focus on defining what constitutes IW, and will examine the utilization and effects of IW during the al-Aqsa Intifada. In order to limit the scope of this study, this thesis will focus on Israeli and Palestinian (to include major supporters of both sides) IW against each other. While this thesis will include psychological operations, deception, and propaganda in its definition of information warfare, the primary focus of this thesis will be the manipulation of electronic impulses, which pose threats to all digitized apparatus within the civilian, military, and governmental sectors. Computer Network Operations are of particular interest.

This thesis will not involve any technical aspects. All research and analysis will be based on documented sources of IW and cyberattacks during the established time period.

D. METHODOLOGY

Primary and secondary sources of research were collected, collated, and analyzed in order to evaluate the utilization and effects of information warfare during the al-Aqsa Intifada. Such sources include newspaper articles, cyber alerts, scholarly journal articles, and threat assessments. Individuals specializing in both the study of the intifadas and information warfare were contacted regarding further sources of information and potential interviews.[1] Contact was made with the Director of Terrorism Studies at the Combating Terrorism Center to obtain further data regarding the utilization and effects of IW during this time period by the designated participants.

This research focuses on defining Information Warfare/Information Operations (IW/IO), identifying the IW capabilities of both Israelis and Palestinians, the use of IW during the al-Aqsa Intifada, and the effects of such IW. In particular, this thesis explores

[1] Dr. John Arquilla, Ph.D., Professor within the Department of Defense Analysis in the Graduate School of Operational and Information Sciences, Naval Postgraduate School. Dr. Dorothy E. Denning, Ph.D., Professor within the Department of Defense Analysis in the Graduate School of Operational and Information Sciences, Naval Postgraduate School. Dr. Ruth M. Beitler, Ph.D., Associate Professor within the Department of Social Sciences, U.S. Military Academy. Dr. James Forest, Ph.D., Assistant Professor within the Department of Social Sciences, Director of Terrorism Studies in the Combating Terrorism Center, U.S. Military Academy.

malicious use of the Internet during the al-Aqsa Intifada. This thesis concludes by exploring attacks, via the Internet, against the U.S. Analysis of the events which have occurred during the “Interfada” and those attacks which have already taken place against the U.S. may be applied to strengthen the United States’ national defense capabilities.[2]

[2] According to InfoWar Monitor, the term ‘Interfada’ was coined in late 2000, after the outbreak of an intense cyberwar pitting Israeli and Palestinian hackers against one another after the outbreak of the Al-Aqsa Intifada and the collapse of the ‘peace-process.’ http://www.infowar-monitor.net/modules.php?op=modload&name=Archive&file=index&req=listarticles&secid=5, last accessed on August 27, 2005.

II. INFORMATION WARFARE/INFORMATION OPERATIONS (IW/IO)

A. INTRODUCTION

Throughout history, the reliance upon information has factored into all forms of warfare. By controlling, manipulating, denying, degrading, and destroying data (and its transmission); forces are able to control information, and thus knowledge. When friendly forces obtain information superiority over their enemy, this knowledge advantage can lead to a better understanding and ability to predict the movements and actions of one's enemy, while at the same time enabling friendly forces to control and manipulate the enemy's perception of the battlefield and/or friendly force intentions. Knowledge, understanding, and rational reasoning/thought, the basic function which differentiates between animals and man, are based solely on the analysis of data. Alone, data are meaningless bits, zeroes and ones, collections without any relevance. When these meaningless bits are analyzed and combined with other bits, they become information. This information enables man to evaluate his environment, the actions which he will take, and potential repercussions of such actions. The ability to manipulate the foundation of information, the bits of data, enables friendly forces to control the adversary's understanding and knowledge of the environment. Examples of information warfare include deception, propaganda, psychological operations, computer network operations, HERF guns, and EMP devices.[3] Such operations have existed since the beginning of time; however, their relevance and increased popularity are due to man's increasing reliance on technology, in particular information technology (IT).

[3] The arsenal of information warfare includes devices for disrupting data flow or damaging entire systems and/or hardware. Included are HERF (High Energy Radio Frequency) guns, which focus a high power radio signal on target equipment, putting it out of action and EMP (Electromagnetic Pulse) devices, which can be detonated in the vicinity of a target system. Yael Shahar, "*Information Warfare: The Perfect Terrorist Weapon*," ICT, (February 26,1997) http://www.iwar.org.uk/cyberterror/resources/CIT.htm, last accessed on May 24,2005.

B. DEFINING INFORMATION WARFARE/INFORMATION OPERATIONS

The economy, businesses, academia, and the greater populous rely upon the Internet for the transfer of funds, goods, ideas, information, et cetera.[4] It is only natural that individuals and/or states will seek to manipulate, degrade, deny, disrupt, and/or destroy the hardware and software upon which governments, militaries, academics, businesses, and the greater populace rely to virtually connect every aspect of life. This growing reliance on technology has resulted in IW evolving into a double-edged sword, which can be utilized by one's enemies: those with the most technologically advanced, and thus reliant, societies most capable of waging IW become the ones most vulnerable to it.

The topic of IW has become increasingly prevalent throughout the government, military, business, and academic sectors of society. A simple Internet search of the topic, using www.google.com, returns 8,190,000 different results; a similar search of Information Operations (IO) returns 146,000,000 results.[5] Government, Department of Defense, academic, and business literature abounds with discussions of the presence, relevance, and threats of so-called "Information Warfare." However, these same institutions, which all too quickly extol the advantages and disadvantages, risks, relevance, and capabilities surrounding this topic, rarely agree upon a single definition. The notion of warfare based on information, i.e., analyzed data which provides knowledge to the user, has become so entrenched that diverse definitions abound. Indeed, there are even various terms used in lieu of, or in addition to, information warfare, including: "infowar," "information operations," "netwar," "command and control

[4] The October 1995 resolution of the US Federal Network Council states that the term 'Internet" refers to "the global information systems logically linked together by a globally unique address space based on the Internet Protocol; it is able to support communications using the Transmission Control Protocol; and it provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and relate4d infrastructure described herein."

[5] www.google.com Google Search: "information warfare" and "information operations," August 19, 2005.

counterwar (C2W)," "Third Wave War," "knowledge war," "information-based warfare," and "cyberwar."[6] According to Giampiero Giacomello,

> 'information warfare' has now been applied to a rather dissimilar (and often incongruent) collection of situations. Its origins can be traced back to the Gulf War, when the UN coalition simply annihilated Iraq's information systems…The current use of the term [sic] has come to include "precision-bombing of enemy's information infrastructure," cyberterrorism and cybercrime, 'script-kiddies,' practicing denial-of-service attacks on commercial Web sites, Web defacement, etc.[7] [8]

The following list provides a few examples of the definitions used to describe IW:

"a coherent and synchronized blending of physical and virtual actions to have countries, organizations, and individuals perform, or not perform, actions so that your goals and objectives are attained and maintained, while simultaneously preventing competitors from doing the same to you."[9]

[6] John Arquilla and David Ronfeldt, of The RAND Corporation, have defined information warfare as being the sum of netwar and cyberwar. Netwar they define as "societal level conflict waged through Internetted modes of communication." Cyberwar they define as "conducting and preparing to conduct military operations according to information principles."

[7] Giampiero Giacomello, *"Measuring 'Digital Wars': Learning From the Experience of Peace Research and Arms Control,"* The Information Warfare Site – Infocon Magazine Issue One, http://www.iwar.org.uk.infocon/ (October 2003).

[8] In an effort to clarify the matter, Arquilla and Ronsfeld (1993) distinguished between "cyberwar" and "netwar" – the latter waged by networked organizations such as terrorist groups, whereas the former deals with state's actions. Alvin and Heidi Toffler's *War and Anti-War: Survival at the Dawn of the Twenty-first Century* (1993) lays the foundations of information war by discussing human history as a series of waves; each wave and its wars based on the means by which wealth is created. The Tofflers posit that the third wave, which we are currently riding, is based on information and, thus, future wars will undoubtedly be waged and won based upon information. Libicki (1995) identified seven "forms" of IW, to include: command and control warfare, which is to separate the enemy's head from the body of his forces; intelligence-based warfare, which consists of measures and countermeasures that seek knowledge to dominate opponents combat power in the battlespace, and combat power potential outside the battlespace; electronic warfare, such as radio-electronic or cryptographic means; psychological warfare, used to influence the minds of friends, neutrals and foes; "hacker" warfare, in which computer systems are attacked; economic information warfare, blocking or channelling information to pursue economic dominance; and cyberwarfare, a futuristic collection of ideas that range from clever to absurd.

[9] Andy Jones, MBE, Gerald L. Kovacich, Ph.D., and Perry G. Luzwick, "Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part I," *Special Issue Coverage: Information Warfare/Cyber-Crime in Information Systems Security* (September/October 2002), 10.

“the physical and computer-based operations used by military forces to compromise the access to and viability of information received by the decision-makers of an enemy, while at the same time protecting their own information and information systems.”[10]

“any action to deny, exploit, corrupt, or destroy the enemy’s information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.”[11]

“a feature of military conflict where information systems are attacked or defended, directly or indirectly as a means to dominate, degrade or destroy, or protect or preserve data, knowledge, beliefs or combat power potential.”[12]

The National Defense University defines infowar as *“the use of information and information systems as weapons in a conflict where information and information systems are the targets.”*[13]

Information-based warfare is *“an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment. Information-based warfare is both offensive and defensive in nature - ranging from measures that prohibit the enemy from exploiting information to corresponding measures to assure the integrity, availability, and interoperability of friendly information assets.”*[14]

The author would like to offer the following as a definition for information warfare: ***Information warfare is the collection, monitoring, exploitation, manipulation, degradation, denial, disruption, corruption, control, and/or destruction of data, its means of collection, and/or its means of transmission in order to attain an information***

[10] “Information Operations,” *Canadian Security Intelligence Service*, http://www.csis-scrs.gc.ca/eng/backgrnd/back9_e.html, (February 2004).

[11] U.S. Department of the Air Force, *Cornerstones of Information Warfare*, 1995.

[12] Charles F. Hawkins, “Coming To Grips with Information Warfare, A Western Perspective,” a HERO Report from the *China Defense Science & Technology Information Center*, March 1997. This is an adaptation of definitions by Col. Richard Szafranski, USAF, and ideas expressed by Gen. Ronald R. Fogleman, U.S. Air Force chief of staff.

[13] Richard W. Aldrich, *The International Legal Implications of Information Warfare*, U.S. Air Force Institute for National Security Studies Occasional Paper 9, http://www.usafa.af.mil/df/inss/OCP/ocp9.pdf, (April, 1996), 3-5.

[14] Working definition recognized by the School of Information Warfare and Strategy of the National Defense University as of 11/16/93.

***advantage over one's adversaries via information superiority and/or perception management and influence during times of conflict/war/aggression in which one side has hostile or nefarious motives*.**

It is important to note that there is little difference between IW and IO; many consider IW simply IO practiced during times of conflict, or the use of IW tools and techniques at any time. In short, IO is defined as actions taken to affect adversary information and information systems while defending one's own information and information systems; IO includes both offensive and defensive elements. IO targets information or information systems (hardware, software, and people) in order to affect the information-based process, whether human or automated. IW is IO conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. In the end, IW is one of the instruments of power that nations wield to influence events and actions during peace and conflict.

C. ELEMENTS OF IW/IO

During the past decade and a half, during which IW/IO have become topics of research, discussion, doctrine, and practice, many officials and scholars have developed lists of IW/IO "core capabilities." These capabilities espouse the levels and abilities to which users are able to monitor, control, and manipulate data, and thus information and knowledge, in the form of broadcast and print media, propaganda, energy impulses, to mention a few. The following list provides the five "core capabilities," and "supporting capabilities" of IW/IO[15]:

1. Psychological Operations (PSYOP)

According to Joint Publication 3-53, Psychological Operations (PSYOP) are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. In most instances, PSYOP is utilized to "influence" the adversary to take

[15] CJSCI 6510.01D (15June2004).

certain actions.[16] According to U.S. Army Civil Affairs and Psychological Operations Command (USACAPOC), PSYOP is the dissemination of truthful information to foreign audiences in support of U.S. policy and national objectives. Persuading rather than compelling physically, PSYOP relies on logic, fear, desire, or other mental factors to promote specific emotions, attitudes, or behaviors. When properly employed, PSYOP can reduce an adversary's will to fight. The intended purpose of PSYOP is to influence the targeted audience to take certain actions based on the information and indicators provided.

2. Military Deception (MILDEC)

According to Joint Publication 3-58, Military Deception (MILDEC) is defined as those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific action (or inaction) that will contribute to the accomplishment of the friendly mission. A key to deception is that the originator does not simply want the adversary to "believe" something, but also wants the adversary to take "action" based upon that belief. MILDEC includes: strategic military deception, operational military deception, tactical military deception, service military deception, and military deception in support of operations security.[17] Joint Force Commanders (JFCs) utilize deception to accomplish their missions by attaining surprise, security, mass, and economy of force. Deception supports military operations by causing adversaries to misallocate resources in time, quantity, place, and effectiveness. The intent of MILDEC is to mislead adversary military/government decision makers, causing them not simply to "believe," but to "take action" based on that belief. During deceptions, friendly forces want their adversaries to be "certain" about friendly intentions, but "incorrect" in their perceptions. Essential to any successful MILDEC operation is a deception story that is believable, verifiable, consistent, and executable. Additionally, the adversary must believe that friendly forces have the means to accomplish whatever action that the deception implies friendly forces will take. The six principles of deception are: focus, objective, centralized control,

[16] Joint Publication 3-53.

[17] Joint Publication 3-58.

security, timeliness, and integration. Deception operations should be an integral component of peacetime and wartime national security.

3. Operations Security

According to Joint Publication 3-54, Operations Security (OPSEC) is defined as a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. OPSEC is a systematic way of viewing friendly operations or activities through the eyes of adversaries, and protect information that is critical to friendly success. OPSEC is an activity that helps prevent adversaries from gaining and exploiting critical information. OPSEC aims to identify any unclassified activity or information that, when analyzed with other activities and information, can reveal protected and important friendly operations, information, or activities. It is a methodology that can be applied to any operation or activity for the purpose of denying critical information to the adversary. Controlling the adversary's access to information by denying or permitting access to specific information can shape adversaries' perceptions; thus, an OPSEC vulnerability may be desired in order to achieve a PSYOP or deception objective. Ultimately, OPSEC seeks to hide truths. The five-step OPSEC process includes: (1) Identify Critical Information, (2) Determine Threat, (3) Assess Vulnerabilities, (4) Weigh Risks, and (5) Apply OPSEC Measures.[18]

4. Electronic Warfare (EW)

According to Joint Publication 3-51, in military operations, the term Electronic Warfare (EW) refers to any military action involving the use of EM or directed energy to

[18] Joint Publication 3-54.

control the EM spectrum or to attack the enemy. EW includes three major subdivisions: Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (ES).[19]

a. Electronic Attack (EA)

EA involves the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Such actions include: prevention and reduction of an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and employment of weapons that utilize either electromagnetic or directed energy as their primary destructive mechanism.20

b. Electronic Protection (EP)

EP involves passive and active means taken to protect personnel, facilities, and equipment from effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.[21]

c. Electronic Warfare Support (ES)

ES involves actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. ES provides critical information for decisions which involve electronic warfare operations, and can be utilized to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence.[22]

5. Computer Network Operations (CNO)

According to U.S. Joint Forces Command, Computer Network Operations (CNO) are comprised of Computer Network Attack (CNA), Computer Network Defense (CND),

[19] Joint Publication 3-51

[20] Joint Publication 3-51.

[21] Joint Publication 3-51.

[22] Joint Publication 3-51.

Computer Network Exploitation (CNE), Computer Network Response (CNR), and Special Information Operations (SIO), collectively.[23]

a. Computer Network Attack (CNA)

CNA involves operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CNA relies on the data stream to execute an attack.[24]

b. Computer Network Defense

CND is defensive measures to protect and defend information, computers, and networks from disruption, denial degradation or destruction.[25]

c. Computer Network Exploitation (CNE)

CNE is intelligence collections and enabling operations to gather data from target adversary automated information systems or networks.[26]

d. Computer Network Response (CNR)

CNR may include measures to determine the source of hostile CNA or CNE.

e. Special Information Operations (SIO)

SIO are information operations that by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the U.S., require a special review and approval process.

Alongside CNO are Information Assurance (IA) and Information Security (INFOSEC).

f. Information Assurance (IA)

IA protects and defends information and information systems by ensuring availability, integrity, identification and authentication, confidentiality, non-repudiation, and provides for restoration of information systems by incorporating protection, detection, and reaction.

[23] U.S. Joint Forces Command (JP 1-02).

[24] Joint Publication 1-02.

[25] Joint Publication 1-02.

[26] U.S. Joint Forces Command.

g. Information Security (INFOSEC)

INFOSEC is the protection and defense of information systems against unauthorized access or modification of information whether in storage, processing, or transit, and against denial of service to authorized users.

Related and Supporting IO Capabilities include: Civil Affairs, Public Affairs, Civil Military Operations, Information Assurance, Physical Security, Physical Attack, and Counterintelligence.

D. U.S. IW/IO DOCTRINE

With regard to U.S. military IW/IO doctrine, all the services are responding to the challenges of the information age. While current concepts of "jointness" require that the services uphold the Joint IO/IW Doctrine, each has developed its own definition and doctrine by which its forces are best able to attain an advantage while denying such an advantage to the enemy via information collection, analysis, dissemination, manipulation, and degradation. The U.S. Marines focus primarily on the human dimension of conflict, with the objective of maximizing human and operational flexibility instead of relying on technology to quell hostilities. The U.S. Army has proven eager to incorporate technology with the human aspects of IO. It has established a number of training commands which investigate the implications of IO/IW concepts and capabilities and publish IO doctrine. The U.S. Navy has practiced elements of IO for decades, and continues to focus/engage in the more technological aspects of IW/IO. It primarily focuses on the command and control warfare elements. Meanwhile, the U.S. Air Force has taken drastic steps to move itself into the information age of warfare. Of all the services, its doctrine expresses the broadest view of IW, stating that information is a "realm" to be dominated. All the services have developed IW centers, which focus on IO concepts, collection, analysis, and dissemination. They recognize that a key element of IO is information superiority; however, their definitions of information superiority differ from one another. Unlike the Navy, Marine Corps, and Army, the Air Force's definition of IO does not incorporate protecting friendly assets/information/information systems from enemy attack. An important point to note, all four services incorporate both offensive and defensive actions as well as the various IO elements, including some form of computer network operations, within their doctrines. Ultimately, while the words are different, the basic meaning behind each service's definition of IO is the same: attain and maintain information dominance over adversaries, while protecting friendly forces and assets against such attacks, and in so doing gain a strategic, tactical, and operation advantage over adversarial forces.

1. U.S. Marine Corps IO Doctrine

U.S. Marine Corps IO Doctrine: According to MCWP 4-40.4, IO includes actions taken to affect the enemy information and information systems while defending friendly information and information systems. The Marine Corps views IO as an integrating concept that facilitates the warfighting functions of C2, fires, maneuver, logistics, intelligence, and force protection. According to the Marine Corps concept of IO, IO can be used to influence peacetime periods by deterring during pre-crisis, enabling during crisis, and restoring during post-crisis across the spectrum of diplomatic, economic, military, and social elements of national power. IO conducted by Marine Air-Ground Task Forces (MAGTFs) will consist primarily of battlespace shaping, force enhancement, force protection actions and any other information-oriented activity that the MAGTF can leverage to better facilitate the application of combat power. In the Marine Corps' perspective, IO is not a warfighting function in its own right; it is an integrating concept that enhances and enables the warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force protection. Thus, the focus of Marine Corps IO will be upon the information-oriented activities that will best support the tailored application of combat power.

2. U.S. Army IO Doctrine

U.S. Army IO Doctrine: According to FM 3-13, IO encompasses attacking adversary C2 systems (offensive IO) while protecting friendly C2 systems from adversary disruption (defensive IO). FM 100-6 defines IO as continuous military operations within the military information environment that enable, enhance, and protect the commander's decision cycle and mission execution to achieve an information advantage across the full range of military operations. IO includes interacting with the Global Information Environment (GIE) and exploiting or denying an adversary's information and decision systems. Effective IO combines the effects of offensive and defensive IO to produce information superiority at decisive points. IO is the employment of the core capabilities of EW, CNO, PSYOP, MILDEC, and OPSEC in concert with supporting and related capabilities to affect or defend information systems, and to influence decision-making. Army doctrine establishes IO as an operational advantage: commanders direct three interdependent contributors to achieve this goal (information management, Intelligence, Surveillance, and Reconnaissance (ISR), and information operations). The goal of IO is to gain and maintain information superiority, a condition that allows commanders to seize, retain, and exploit the initiative.[27] Prior to JP 3-13, the Army routinely employed elements of IO. The Gulf War demonstrated the benefit of utilizing these elements in concert with one another and in synchronization with ground operations. The major elements of Army IO include: IO are continuous, conducted both during peacetime and war; Army IO involves interacting within the GIE, while operating in the military information environment; Army IO focuses on the decision cycle, supporting more informed decision-making by friendly commanders, while denying the enemy decision-maker full use of his decision cycle through IO attacks; and the goal of Army IO is to achieve an information advantage over the adversary. Army IO doctrine consists of three parts: intelligence and other relevant information, information systems, and command and control warfare.

The Army's IO doctrine goes beyond the joint military strategy of command and control warfare. It integrates a broader approach to the impact of information on ground operations. Additionally, unlike the joint doctrine, Army IO doctrine recognizes that the various elements of IO can be used both offensively and defensively. Of particular interest, the Army's doctrine, unlike joint doctrine, defines IO as "the actions that target adversaries' information systems as well as influence others' decision-making processes, information and information systems…" This definition illustrates that the Army recognizes that various groups of actors, including NGOs, refugees, civil and military authorities, the populace, etc. may significantly impact a commander's plans if their motives, needs, and presence are not recognized and addressed during military

[27] According to FM 3-13, information superiority is defined as the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

operations. A point of particular interest within the Army's IO doctrine is the incorporation of the commander's intent and decision-making capabilities. The Army clearly illustrates that the purpose of IO is to provide an advantage to our forces while denying such advantages to our adversaries, and in so doing provide our decision-makers with the best information and capabilities to develop courses-of-action and implement said actions.

3. U.S. Navy IO Doctrine

U.S. Navy IO Doctrine: According to OPNAV 2201.2, the discipline of information operations (IO) and its subset of information warfare (IW) encompass not only actions that may be taken to potentially affect an adversary's information or information systems, but also address those defensive aspects necessary to ensure that U.S information and information systems are protected against attack. Sea Power 21 predicts that the importance of information operations (IO) as an element of the Sea Strike concept will only increase as high-tech weapons and systems, particularly advanced information technologies, become more widely available. According to the former Chief of Naval Operations, ADM Vern Clark, USN; "Information operations will mature into a major warfare area, to include electronic warfare, psychological operations, computer network attack, computer network defense, operations security, and military deception. Information operations will play a key role in controlling crisis escalation and preparing the battlefield for subsequent attack."[28]

4. U.S. Air Force IO Doctrine

U.S. Air Force IO Doctrine: According to AFDD 2-5 (2004), the Air Force believes that IO comprises those actions taken to gain, exploit, defend, or attack information systems in the broadest context of those terms. These actions (gain, exploit, defend, and attack) may occur simultaneously. For airmen, IO includes both Information-In-War (IIW) and Information Warfare (IW). IIW relates to the gain and exploit aspects of IO and supports all air and space functions, including IW, across all phases of operations. IW relates to the attack and defend aspects of IO, and it also

[28] Admiral Vern Clark, USN. "Projecting Decisive Joint Operations." *Proceedings*, U.S. Naval Institute: October 2002, http://www.usni.org/Proceedings/Articles02/PROcno10.htm, last accessed on September 23, 2005.

supports all air and space functions across all phases of operations. Both IW and IIW are conducted throughout all phases of an operation and across the range of military operations. IO target information, or information systems, in order to affect the information-based process, whether human or automated. IO are those operations that achieve and maintain information superiority, that degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition. In turn, information superiority is a key component of air and space superiority. Air Force doctrine recognizes a fully integrated spectrum of military operations. Revisions to Air Force IO doctrine (AFDD 2-5, 2005), replaced the terms IIW and IW with three distinct groups of capabilities that form the foundation of the new definition of IO. "Information Operations…are the integrated employment of the capabilities of influence operations, electronic warfare operations, and network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."

III. COMPUTER NETWORK OPERATIONS: DIGITAL WARS

Cybercrime/Cyberwarfare/Cyberterrorism/Cyberattacks

Manipulations and Fraudulent use of Computer Network Systems, the Internet, and Modes of Transmission

> We are at risk…[Computers] control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to businesses plans to criminal records. Although we trust them, they are vulnerable – to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.[29]

A. INTRODUCTION

An increasingly important element of IW is CNO. CNO comprises offensive and defensive aspects, including active and passive operations, and security measures. Such operations are conducted by governments, militaries, businesses, and regular citizens. The growing reliance on computers, computer network systems, and the Internet has fueled the transmission of ideas, the growth of economy, and the means of communication throughout the world. Unfortunately, individuals and groups, both state and non-state actors, have utilized computers and their networks with less than friendly motives. "Cyberwarfare" and "cyberterrorism" are often used as umbrella terms for electronic attacks that are not merely criminal in nature, such attacks fall in the realm of CNO. Individuals, organized groups, nations, and states involved in domestic and international conflicts can, and have, used computer networks to spread propaganda, unite efforts, secure communications, gather intelligence, manage funds, and launch attacks. Today, contemporary databases and multiple channels for information transmission have created the opportunity for custom-tailored netwar attacks. Examples of entry points and dissemination networks for such attacks include: computer bulletin boards, chat rooms, e-mail, cellular telephones, and video cameras tied to fax machines

[29] National Research Council, "Computers at Risk" National Academy Press, 1991.

and/or computer systems.[30] Examples of attacks include: online fraud (or "phishing"), "sniffing," espionage, sending viruses, computer or network penetration, denial-of-service attacks on computers and networks, sensor jamming, manipulation of trusted information sources, and even the threat of "cyberterrorism." Such "cyber attacks might be referred to as hacking, cyber mischief, cyber hooliganism, personal or corporate theft, revenge, or espionage, or organized crime activities (foreign and domestic)."[31] This form of "warfare" appeals to many because it is a low-cost, generally high profile, and difficult to trace alternative to initiating physical violence.[32] According to the 2001 CRS Report for Congress, cyberwarfare "provides a range of relatively anonymous, non-lethal options that can be applied at the speed of light with relatively low risk of escalation to more direct forms of conflict. In one sense, it's a way for others to wage an asymmetrical conflict…"[33]

The use of computers, computer networks, and the Internet to inform, persuade, or deny audiences access to information is becoming "…almost standard practice in any political conflict…"[34] The combination of relatively inexpensive means of warfare, a computer and Internet access, free online weapons and tactics, and the lack of national

[30] George J. Stein, "Information War – Cyberwar – Netwar," in Battlefield of the Future: 21st Century Warfare Issues, http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html, last accessed on August 11, 2005.

[31] Steven A. Hidreth, "Cyberwarfare," CRS Report for Congress, p. 3, updated June 19, 2001, http://www.fas.org/irp/crs/RL30735.pdf, last accessed on August 28, 2005.

[32] The terms "cyberwar" and "netwar" were coined by John Arquilla and David Ronfeldt while employed with the International Policy Department at the RAND Corporation. According to their publications, cyberwar refers to knowledge-related conflict at the military level, and netwar applies to societal struggles most often associated with low intensity conflict by non-state actors. Both concepts imply that future conflicts will be fought more by "networks" than by "hierarchies," and that whoever masters the network form will gain major advantages. Further reading on this topic includes: John Arquilla and Dovid Ronfeldt, "Cyberwar is Coming!," Journal of Comparative Strategy, Vol. 12, no. 2, pp 141-165 (1993), John Arquilla and David Ronfeldt, Networks and Netwar: The Future of Terror, Crime and Militancy, RAND (2001), http://www.fathom.com/course/21701735/, last accessed on August 28, 2005. Throughout this thesis, the terms "cyberwar," "cyberwarfare," and "netwar" will not follow the definitions provided by Arquilla and Ronfeldt, but will instead align with the more general use which commonly equates these terms with electronic attacks on computers, computer network systems, the Internet, and modes of transmission.

[33] Steven A. Hidreth, "Cyberwarfare," CRS Report for Congress, p. 2, updated June 19, 2001, http://www.fas.org/irp/crs/RL30735.pdf, last accessed on August 28, 2005.

[34] John Schwartz, "When Point and Shoot Becomes Point and Click," *The New York Times: On the Web*, November 12, 2000, http://www.twurled-world.com/Infowar/Update3/URL_Details/URL_287.htm, last accessed on August 12, 2005.

boundaries makes cyberwarfare an effective weapon of choice for individuals and groups (acting alone and/or at the behest of the state) seeking to inform societies, spread propaganda, deny service to their enemy's, and potentially destroy critical infrastructures.[35] According to David J. Farber, an Internet pioneer who serves on the board of the Electronic Frontier Foundation, an online civil liberties group, as dependency on the Internet increases, cyberwarriors will do real damage and at some point somebody will get the brilliant idea, "Why bomb them? Why not cyberbomb them?"[36] This notion is further espoused by Giampiero Giacomello, who insists that CNO have the potential to satisfy the "break things and kill people" (BTKP) rule.[37] [38] [39]

B. TYPES OF CYBERWARFARE, POTENTIAL "INFOWAR" WEAPONS, CYBERWARFARE TOOLS, AND CYBERWARFARE TACTICS

1. Types of Cyberwarfare[40]

- Web Vandalism - the deactivating and/or defacing of Web pages; hackers break into a website's files and alter them by posting obscenities or generally changing the content of the site that is viewed on the World Wide Web

[35] According to the U.S. Critical Infrastructure Assurance Office (CIAO), "critical infrastructures" are "those systems and assets – both physical and cyber – so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety." Originally, the Presidential Decision Directive, PDD-63 of May 1998, http://www.fas.org.irp/offdocs/pdd/pdd-63htm, identified eight sectors as "critical." Since then, these eight have been reorganized, and currently, the sectors identified as "critical" are: information and communications, electric power, transportation, oil & gas, banking & finance, water, and emergency services. The concept and definition of critical infrastructures is further espoused in the U.S.A PATRIOT Act, approved by Congress in October 2001.

[36] Ibid.

[37] Giampiero Giacomello, "*Measuring 'Digital Wars': Learning From the Experience of Peace Research and Arms Control,*" The Information Warfare Site – Infocon Magazine Issue One, http://www.iwar.org.uk.infocon/ (October 2003). According to Giacomello, if CNO were valuable only to disrupt enemy's C4I systems, it would only qualify as a new tool for EW, a force multiplier for kinetic weapons. However, because it is possible that CNO could cause mechanical failures leading to the loss of human lives or considerable economic damage, it possesses the potential to fulfill the "break things and kill people" rule considered by military planners.

[38] John Arquilla, "The Great Cyberwar of 2002," Wired Magazine, July 10, 2002, http://hotwired.wired.com/collections/future_of_war/6.02_wyberwar_2002_pr.html, last accessed on August 11, 2005. In "The Great Cyberwar of 2002," John Arquilla provides a real-life scenario of the threats, actions, and results of cyberwar.

[39] Gregory J. Rattray, Strategic Warfare in Cyberspace, The MIT Press, Cambridge, MA, 2001. This book provides a detailed discussion of strategic warfare in cyberspace.

[40] "Types of Cyberwarfare" according to "Special Focus: Cyberwarfare," The Center for the Study of Technology and Society, http://www.tecsoc.org/natsec/focuscyberwar.htm, last accessed on May 24, 2005.

- Disinformation Campaigns - the Internet is a popular tool for finding news, and can be utilized to spread mis- and dis-information to affect a population's beliefs or psychology; additionally, the Internet can be used as an open forum and platform for rhetoric to incite sympathizers

- Gathering Secret Data - classified and sensitive information which is not handled securely can be intercepted and/or tampered, i.e. computer network espionage

- Disruption in the Field/Denial of Service - individuals can block, intercept, or pollute vital lines of communication; this form of attack is of particular importance to the military which relies heavily upon electronic communications, transmitted via computers and satellites, to coordinate activities; such attacks can be carried out by flooding a site with e-mail or overwhelming it with requests for information which block others' access to the site and/or cause the site to crash

- Attacking Critical Infrastructure - many components of the national critical infrastructure (electricity, water, fuel, communications, transportation) are vulnerable to concerted electronic attacks; such attacks pose serious domestic disasters, including financial meltdown, flooding, chaos, and mass casualties

2. Potential Weapons[41]

- Computer Viruses - can be fed into a computer either remotely or by "mercenary" technicians

- Logic Bombs - a type of computer virus which can lie dormant for years, until, upon receiving a particular signal, is awoken and begins attacking the host system

- Chipping - a plan (originally proposed by the CIA, according to some sources) to slip booby-trapped computer chips into critical systems sold by foreign contractors to potentially hostile third parties and/or recalcitrant allies

- Worms - self-replicate ad infinitum, eating up a system's resources

[41] "Potential Infowar Weapons" according to Yael Shahar in "Information Warfare: The Perfect Terrorist Weapon," February 26, 1997, http://www.iwar.org.uk/cyberterror/resources/CIT.htm, last accessed on May 24, 2005.

- Trojan Horses - a malevolent code inserted into legitimate programming in order to perform disguised functions
- Back Doors and Trap Doors - a mechanism built into a system by the designer, in order to provide the manufacturer or others the ability to “sneak back into the system” at a later date by circumventing the need for access privileges

3. Cyberwarfare Tools[42]

- Social Engineering
- Hacking
- Denial-of-Service attacks
- Eavesdropping
- Dumpster Diving
- Identity Theft
- Sabotage
- Insertion of rogue code
- Industrial Espionage
- Stealing intellectual property and confidential information
- Physical Theft
- Insertion of misinformation
- Perception Management

4. Cyberwarfare Tactics[43]

- Eavesdropping on the opponent’s/target’s computer networks and communications
- Interrupting transmission of messages across adversary’s communications lines

[42] Helen Armstrong and John Davey, “Educational Exercises in Information Warfare – Information Plunder and Pillage,” Submitted to NCISSE 2001, May 22-24, 2001, 5th Annual Colloquium for Informatioin Systems Security Education, George Mason University, http://cisse.info/CISSE%20J/2001/Arms.pdf, last accessed on August 29, 2005. The authors state that these are potential tools used cyberwar attacks.

[43] Ibid. Armstrong and Davey provide these examples as possible tactics used in cyberwarfare. This list is not meant to be an exhaustive one.

- Intercepting and altering messages being transmitted between management and operations
- Mapping the opponent’s network
- Scanning the opponent’s networks for vulnerabilities
- Providing misinformation to confuse the opponent
- Planting fast acting rogue code on the opponent’s system (i.e. viruses, worms, etc.)
- Using known vulnerabilities in software to gain access to the opponent’s system
- Planting bad data or code to surreptitiously undermine the opponent’s systems or data
- Launching denial-of-service attacks against the opponent
- Ensure accurate reporting of happenings, i.e. report only facts
- Monitoring own systems for intrusions, eavesdropping, mapping, and scanning
- Analyze the opponent’s patterns of attack for pre-empting future actions and attacks
- Attacking from bogus, anonymous, or innocent sources/servers
- Penetrating computer networks
- Reconfiguring the opponent’s firewall
- Planting spies in opponent’s operations (i.e. insiders, disenfranchised employees, contractors)
- Monitoring own transactions for spies
- Having imaged backups of computing software and environment to allow fast recovery
- Ensuring backup hardware and power supply are on hand
- Develop efficient command and control systems
- Ensure all members know their area of responsibility and boundaries for decision-making
- Ensure all members know the procedures and rules

- Ensure all members have an in-depth knowledge of their tools and tactics
- Debrief regularly

C. ACTIVISM, HACKTIVISM, AND CYBERTERRORISM[44]

The CNO undertaken by individuals, groups, nations, and states, whether alone or with state support, generally fall into one of three categories: activism, hacktivism, and cyberterrorism, according to Dorothy E. Denning. The Internet offers an available and inexpensive media for collecting and publishing information, for communicating and coordinating action on a global scale, for banking and shopping, for educating, and for persuading, influencing, and challenging individuals, groups, and/or governments. The open forum provided by the Internet has evolved into an outlet used by many to promote and participate in activism, draw attention to "worthy" causes, and possibly inflict grave harm in an attempt to influence perceptions and/or policies. Such an environment possesses potential as an effective means of deterrence and/or aggression between state and non-state actors during times of conflict.

1. Activism

> The arrival of the Internet has provided the first forum in history for all the disaffected to gather in one place to exchange views and reinforce prejudices. It is hardly surprising, for example that the right-wing militias' favorite method of communication is e-mail and that forums on the Internet are the source of many wild conspiracy theories that drive the media.[45]

According to Denning, "activism refers to normal, non-disruptive use of the Internet in support of an agenda or cause."[46] Such use includes: browsing the World Wide Web for information, creating websites and posting materials on them, communicating via e-mail, and participating in discussions via chat rooms, bulletin boards, and instant messaging. The extent to which the Internet is available and in use

[44] Dorothy E. Denning has been credited with classifying Internet use and attacks into three categories: activism, hacktivism, and cyberterrorism in "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," Nautilus Institute, http://www.iwar.org.uk/cyberterror/resources/denning.htm, last accessed on August 27, 2005.

[45] Adams Janes, "Clinton's Dreams Die a Dirty Death," The Sunday Times, London, July 27, 1997.

[46] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, http://www.nautilus.org/info-policy/workshop/papers/denning.html, last accessed on August 27, 2005.

(according to Nua Internet Surveys as of September 2002 there were 605.60 million users worldwide) enables individuals and groups from vast geographic regions to communicate and interact with one another with the click of a mouse. Such availability makes it relatively easy to spread ideas, coordinate action, and ultimately influence perceptions and/or policies. Denning describes five modes of using the Internet which fundamentally support the role and goals of activists:

- Collection – there are numerous tools that help with collection, including: search engines, e-mail distribution lists, chat and discussion groups, and Web-based tutorials and training
- Publication – the Internet offers various channels whereby individuals, groups, nations, and states can publish information (and disinformation), including: use of e-mail, posting to newsgroups, creating electronic publications, contributing articles and essays to electronic publications, maintaining online journals and/or "blogs," establishing Web pages with documents, images, audio and video clips, and participating on bulletin boards and in chat rooms
- Dialogue – the Internet offers several venues for dialogue and debate, including: e-mail, newsgroups, Web forums, chat rooms, and discussion boards
- Coordination of Action – the Internet can be utilized to coordinate action between individuals, among members within groups, among members between groups, and organizations; the use of e-mail and Web sites to distribute action plans provides a faster, cheaper, more extensive, and relatively secure medium to deliver messages and information
- Lobbying Decision Makers – whether or not solicited, activists utilize the Internet to influence and lobby decision makers, whether thru direct communication or influencing the greater populace; such methods include: the use of propaganda, e-mail campaigns, electronic petitions, and letter writing campaigns

2. Hacktivism

According to Denning, "hacktivism is the convergence of hacking with activism, where "hacking" is used here to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software ("hacking tools")."[47] Due to the nature of such actions, hacktivism often generates considerable publicity for both the activists and their causes. Denning explores four types of operations within this category:

- Virtual Sit-Ins and Blockades – the cyberspace version of a physical sit-in or blockade; the goal in both cases is to call attention to the "protestors" and their cause by disrupting normal operations and blocking access to facilities; "activists" visit a website and attempt to generate so much traffic that legitimate users are unable to access the site due to bandwidth constraints[48]
- E-Mail Bombs – bombarding a server with multiple messages simultaneously, distributed with the aid of automated tools; the effect can be to completely jam a recipient's incoming e-mail box, making it impossible for legitimate e-mail to get through; due to their nature, e-mail bombs are a form of virtual blockade
- Web Hacks and Computer Break-Ins – "hackers" gain access to websites and erase, replace, and manipulate the content; additionally, hacktivists are able to alter what viewers see when they visit a website by tampering with the Domain Name Service so that the site's domain name resolves to the IP address of another site (when users point their browsers to the intended site, they are redirected to the alternate site)
- Computer Viruses and Worms – hacktivists have used computer viruses and worms to spread protest messages and to damage target computer systems; both are forms of malicious code that infect computers and propagate over

[47] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, http://www.nautilus.org/info-policy/workshop/papers/denning.html, last accessed on August 27, 2005.

[48] There are a variety of methods whereby an individual, acting alone, can disrupt or disable Internet servers. These frequently involve using attack software that floods the server with network packets. When large numbers of individuals simultaneously attack a designated site, the operations is often referred to as "swarming." Swarming can amplify other types of attack, for example, a ping attack or an e-mail bombing. The notion of swarming is discussed by John Arquilla and David Ronfeldt.

computer networks; viruses, especially those carrying destructive payloads, are a potentially potent tool in the hands of cyberterrorists[49]

3. Cyberterrorism

> The potential for physical conflict to be replaced by attacks on information infrastructures has caused states to rethink their concepts of warfare, threats and national assets, at a time when information is recognized as a national asset. The adoption of new information technologies and the use of new communication media, such as the Internet, create vulnerabilities that can be exploited by individuals, organizations, and states.[50]

> Cyberterrorism has evolved into more than just kiddie hackers and the odd denial-of-service attack. It's a phenomenon that can affect the course of a conflict and the minds of the public – and must be addressed.[51]

In the 1980s, Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term "cyberterrorism" to refer to the convergence of cyberspace and terrorism.[52] Mark Pollitt, special agent for the FBI, offers the following as a working definition: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents."[53] Denning claims that cyberterrorism "is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives…to qualify as cyberterrorism, an attack should result in violence against person or property, or at least cause enough harm to

[49] A worm is an autonomous piece of software that spreads on its own, whereas a virus attaches itself to other files and code segments and spread through those elements, usually in response to actions take by users (i.e. opening an email attachment).

[50] Canadian Security Intelligence Service 1996 Public Report, Part IV, Information Technology, http://www.csis-scrs.gc.ca/eng/publicrp/publ1996_e.html#5, last accessed on August 27, 2005.

[51] Quote from the organizers of the "Battle of the Servers, Battle of the Hearts" symposium, found in "Israel's Seminar on Cyberwar," by Tania Hershman, Wird News, January 10, 2001, http://www.wired.com/news/politics/0,1283,41048,00html, last accessed May 26, 2005.

[52] Barry Collin, "The Future of Cyberterrorism," Crime and Justice International, March 1997, p. 15-18.

[53] Mark M. Pollitt, "Cyberterrorism – Fact or Fancy?," Proceedings of the 20th National Information Systems Security Conference, October 1997, p. 285-289, http://www.cs.georgetown.edu/~denning/infosec/pollitt.html, last accessed on August 27, 2005.

generate fear."[54] Attacks which cause serious harm, such as severe economic hardship, sustained loss of power or water, and loss of life, are characterized as cyberterrorism.

With international dependence on computers, computer network systems, and the Internet, the threat of a terrorist-level attack on computers and computer networks possesses the potential to effect as much harm on military and civil society as bombs and guns. The use of viruses, such as ILOVEYOU, has been estimated to have hit tens of millions of users and cost billions of dollars in damage. The following provides examples of malicious use of the Internet across borders: in March 1994, Datastream Cowboy, a 16 year-old British student, was fined after pleading guilty to attacking the Air Force Rome Lab in New York; in 1994, hackers from St. Petersburg and Moscow, Russia virtually broke into Citibank and stole more than $400,000; in 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period with messages that read "We are the Internet Black Tigers and we're doing this to disrupt your communications"; in February 2000, denial-of-service attacks against Yahoo, CNN, eBay, and various other e-commerce websites was estimated to have caused over a billion dollars in losses. While these examples illustrate the effectiveness of cyberwarfare to disrupt, deny, degrade, manipulate, and exploit computers and computer networks, financial institutions, governments, communications capabilities, and businesses, they fail to call to mind the horrendous acts usually associated with terrorism. However, it is only a matter of time before terrorists utilize the Internet and computer network systems to inflict chaos and mass casualties upon innocent societies:

a. Cyberterror Scenarios

Collin suggests a number of scenarios in which computers and computer networks can be utilized by terrorist elements:[55]

- A cyberterrorist hacks into the process control computers on a cereal manufacturing line and alters the levels of iron supplement added to a fatal dose. As a result, boxed cereal sickens and kills children throughout a nation.

[54] Dorothy E. Denning, "Cyberterrorism," Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May, 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, last accessed on August 27, 2005.

[55] Barry Collin, "The Future of Cyberterrorism," Crime and Justice International, March 1997, p. 15-18.

- A cyberterrorist either obtains control of the air traffic control system or alters the system in such a fashion that airplanes are flown into each other, resulting in mass casualties.
- A cyberterrorist either obtains control or alters the control system responsible for the operation of a subway or train system, resulting in mass casualties.
- A cyberterrorist disrupts banks, international financial transactions, and stock exchanges. As a result, economic systems grind to a halt, the public loses confidence, and destabilization is achieved.

Other scenarios could include:

- Use of the Internet for funds transfer and Internet fraud to provide financial backing for terrorist organizations and activities.
- Use of the Internet to plan and coordinate terrorist attacks.
- Attacks on the networks of hospitals resulting in the fatal distribution of incorrect medicines to patients.
- Attacks on the control systems for power grids, water management facilities, and communications systems.
- Attacks on control systems and communication capabilities of emergency response units.

b. The Threat

Are there targets that are vulnerable to attack that could lead to violence or severe harm? Without a doubt, there are sufficient targets of attack that could lead to violence and/or severe harm. The aforementioned scenarios provide a few examples in which the disruption, degradation, manipulation, denial, and/or exploitation of computers, computer networks, the Internet, and modes of transmission and communication could easily result in mass casualties. Members of the government, defense, academic, and business sectors have indicated the vulnerabilities inherent to dependence on computers and computer networks. Even with humans-in-the-loop, the vulnerabilities of computers and networks provide those with nefarious motives ample opportunity to utilize viruses, backdoors, swarming, Trojan horses, malicious code, and denial-of-service to attack key nodes of critical infrastructure, resulting in mass casualties and economic catastrophe. Such an attack has been referred to as "an electronic Pearl Harbour."

c. The Actors

Are there actors capable and motivated to carry out cyberterrorism? In August 1999, the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California issued a report entitled "Cyberterror: Prospects and Implications." In this report, the participants concluded that the barrier to entry for anything beyond annoying hacks is quite high, and that terrorists generally lack the wherewithal and human capital needed to mount a meaningful operation. Of the five terrorist group types examined, the study determined that "the most dangerous eventuality will likely come from a newly formed, religious group."[56] Despite this conclusion, a year earlier, Clark Staten, executive director of the Emergency Response & Research Institute in Chicago, testified that it was believed that "members of some Islamic extremist organizations have been attempting to develop a "hacker network" to support their computer activities and even engage in offensive information warfare in the future."[57] More recently, in February 2004, General John Gordon, the White House Homeland Security Advisor, indicated that whether someone detonates a bomb that causes bodily harm to innocent people or hacked into a web-based IT system in a way that could, for instance, take a power grid offline and result in a blackout, the result is ostensibly the same. He also stated that the potential for a terrorist cyber attack is real.[58] The planning, coordination, and funding for the September 11, 2001 terrorist attacks on the World Trade Center, which were carried out by members of the terrorist organization

[56] "Cyberterror: Prospects and Implications," Center for the Study of Terrorism and Irregular Warfare, Monterey, CA prepared for the Defense Intelligence Agency, October 1999, http://www.nps.navy.mil/ctiw/files/Cyberterror%20Prospects%20and%20Impications.pdf, last accessed on August 30, 2005.

[57] Clark L. Staten, "Foreign Terrorism in the United State: Five years After the World Trade Center," testimony before the Subcommittee on Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee, February 24, 1998, http://www.emergency.com/senate98.htm, last accessed on August 30, 2005.

[58] Mudawi Mukhtar Elmusharaf, "Cyber Terrorism: The New Kind of Terrorism," Computer Crime Research Center, April 8, 2004, http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism, last accessed on August 18, 2005.

al-Qaeda, have been tied to use of the Internet.[59] According to Rabbi Abraham Cooper, deputy director of the Simon Wiesenthal Center in Los Angeles, "The truth is, the terrorist groups, al-Qaeda and those affiliated with it, use every available part of the Internet to promote their agenda…That includes command and control – sending encrypted messages thousands of miles to their operatives."[60] Additionally, the attacks themselves, not counting lives lost and damage to infrastructure and morale, almost blocked (and certainly slowed down) Internet traffic between Europe and the United States for almost two days, and delivered a blow to financial markets.[61] Furthermore, according to Senator Jon Kyl, Chairman of the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security; members of al-Qaeda have tried to target the electric power girds, transportation systems, and financial institutions.[62] Though it remains unknown whether it was a terrorist act or not, the blackout of the northeastern United States and eastern Canada in August 2003, which affected an estimated 10 million people in Canada and 40 million people in the U.S. and produced estimated losses of $6 billion, reflects the type of damage that would result from a cyber attack to critical infrastructure. As a final note, according to Gabriel Weimann, a professor at the University of Haifa in Israel, there are 4,300 terror-related websites worldwide; this fact alone indicates that terrorist organizations are capable and motivated to use the Internet to recruit members, raise funds, spread ideologies, and affect change via legal and illegal means.

[59] Emerson, Steven . American Jihad: The Terrorists Living Among US. New York: The Free Press, 2002.

[60] Alan D. Abbey, "Virtual Jihad," The Jerusalem Post, May 8, 2004, posted on Information Warfare Monitor, http://www.infowar-monitor.net, last accessed August 28, 2005.

[61] One of the backbone cables which supported Internet traffic between the United States and Europe passed under the World Trade Center.

[62] Mudawi Mukhtar Elmusharaf, "Cyber Terrorism: The New Kind of Terrorism," Computer Crime Research Center, April 8, 2004, http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism, last accessed on August 18, 2005.

d. Why Terrorists Utilize Computers, Networks, and the Internet

The Internet has become a virtual "safe-house" for terrorist, extremists, and their targeted audiences. The use of computers, networks, and the Internet has enabled sub-state and semi-detached terrorists the ability to network and inter-connect to find allies and influence audiences. Information and Communication Technologies (ICTs) have enabled multiple leaders to coordinate actions and act parallel to one another despite various international locations. Geographical dispersion, both physical and virtual, provides extra security, and enables terrorists to carry out communication, coordination, and attacks with little worry of interception and/or retribution. The extent to which terrorists have utilized the Internet can be viewed on the Search for Terrorist Entities (SITE) Institute's website, which includes terrorists' daily communications, militant communiqués, militant manuals, terrorist publications, and links to terrorist websites.[63]

- ICTs allow interconnectivity, i.e. communication and networking, both externally and internally. For example, the website for Hezbollah has published a daily diary of the terrorist attacks its members have carried out in southern Lebanon, and the site urges contact from anybody with an opinion about the organization's anti-Israel activities. A spokesman stated, "The service is very important for the morale of our resistance fighters. They are always happy to know that people around the world are backing them."[64]
- Cyberspace allows covert communication and anonymity. Hamas is known to conceal its communications, and its use of electronic messages has presented problems for security agencies. Additionally, a number of Islamist sites provide password-protected communications to members and close sympathizers. Steganography, the art of embedding coded information in anything from photographs to MP3 sound files, has been utilized by terrorists to communicate with one another and plan attacks without having their messages intercepted and/or deciphered.

[63] http://www.siteinstitute.org/index.html, last accessed on August 30, 2005.

[64] "Hizbollah on the Internet," *The Daily Telegraph*, London, February 19, 1997.

- The Internet is inexpensive and virtually omnipresent. For the price of a computer and modem or for a session in an Internet café, extremists and terrorists can become active participants in domestic and international events. The use of small, cheap laptop computers in storing terrorists' plans was illustrated by Ramzi Ahmed Yusuf, the mastermind of the 1993 World Trade Center bombing, who utilized his computer to work out operational plans to bomb American airlines in the Pacific.
- ICTs act as a force multiplier, providing terrorists with reach and influence that was previously reserved for well organized, state-funded terrorist organizations. ICTs have eliminated the borders that once separated exiled leaders from their flocks and attackers from their targets.
- ICTs enable terrorists to reach their target audiences when other outlets and media are denied them. For example, when television networks in the U.S. did not air the beheadings of American and allied hostages during Operation Iraqi Freedom, terrorists ensured that video clips were available for their audience's viewing via various websites.

IV. PALESTINIAN-ISRAELI “INTERFADA”[65]

A. INTRODUCTION AND BACKGROUND

The Middle East conflicts over the past half century are a direct result of the division of the former British mandate of Palestine and the creation of the state of Israel at the end of World War II. The Zionist movement, whose aim was the establishment of a homeland for the Jews scattered around the world as a result of the Diaspora, culminated in the creation of Israel in 1948. Since its creation, Israel has been a region plagued by conflict between the state of Israel and the Palestinians, represented by the Palestine Liberation Organization (PLO), the Palestinian Authority (PA), Israel’s Arab neighbors, and numerous pro-Palestinian organizations (i.e., HAMAS, the Palestinian Islamic Jihad, and the Palestinian National Liberation Movement “Fateh”). During this time, hundreds of thousands of Palestinians have been displaced and several wars have been waged involving Egypt, Jordan, Syria, and Lebanon. Since 1967, Palestinians in Gaza and the West Bank, including East Jerusalem, have lived under Israeli occupation. Until recently, when Israel closed all its settlements in the Gaza Strip and four in the West Bank, the Israeli settlements were home to approximately 400,000 people in the West Bank and were deemed illegal under international law. In 1978, Israel and Egypt entered into the Camp David Accord, which led to normalization of diplomatic relations between Egypt and Israel for the first time since Israel was declared an independent state. Although the “Framework for Peace in the Middle East” was never implemented, Israel agreed to return the territory captured during the Six-Day War in return for Egypt’s recognition of Israel as a nation. In 1993, Mahmoud Abbas, representing the Palestine Liberation Organization, and Shimon Peres, representing the state of Israel, signed the Oslo Accords which were a culmination of a series of secret and public agreements, dating particularly from the Madrid Conference of 1991 onwards, and negotiated between the Israeli government and the Palestine Liberation Organization (acting as

[65] The information contained in this section is directly attributed to the 2001 iDefense Intelligence Services Report on the Israeli-Palestinian Cyber Conflict, Sean Lawson’s “The Cyber-Intifada Resource Guide,” and a plethora of reports, articles, and alerts. Appendix A contains a complete listing of all sources utilized during the research, analysis, and construction of this section; sources are listed chronologically. All quotes are taken directly from these documents, and they include all spelling and grammatical errors.

representatives of the Palestinian people) as part of a peace process trying to resolve the Palestinian-Israeli conflict. Despite concessions and formal agreements, tensions between Israel and Arabs continues throughout the region, with the most recent conflicts including the First Intifada, the al-Aqsa Intifada, and the tensions surrounding the Israeli settlements.

1. The First Intifada

In the months leading up to the First Intifada, numerous events occurred that increased hostilities between the Palestinians and the Israelis. On October 1, 1987, Israeli military forces ambushed and killed seven men from Gaza believed to be members of the Palestinian Islamic Jihad. Several days later, an Israeli settler shot a Palestinian schoolgirl in the back. Palestinian militants attacked and killed innocent Israeli citizens as well as Israeli soldiers. Riots escalated throughout the occupied territories, and were particularly severe in the Gaza Strip. The First Intifada erupted on December 9, 1987 in the Israeli-occupied Palestinian Territories. The immediate cause of the uprisings was a vehicular accident, which killed four Palestinians in the Gaza Strip, sparking immediate protests that rapidly spread to the West Bank. However, the deeper roots of the uprising can be found in the poor economic conditions and harsh military rule of the Israelis who have occupied the Palestinian Territories since 1967. Stone throwing and the use of home-made explosive devices on behalf of the Palestinians, and the use of tear gas, rubber bullets, and the demolition of Palestinian homes by Israeli troops marked the violence which would become known as the "First Intifada." These choices of weapons indicate the disparity between Israel's modern military might and the Palestinian's relatively weak and unorganized establishment. Although the PLO was exiled in Tunis, and thus unable to control the day-to-day events in the Palestinian Territories, it quickly took matters into its hands, sponsoring riot provocateurs and enhancing their presence in the territories that was to guarantee the continuation of the riots. The main leadership role of the uprising was filled by the United Leadership of the Uprising (UNLU), an anonymous group of local Palestinians with little direct connection to the PLO.[66] In

[66] W. Sean McLaughlin, "E-Intifada: Internet in the Palestinian Uprising," *Foundations*, 2001-2002.

addition, Hamas and the Palestinian Islamic Jihad played a crucial role in inducing further violence into the area.

Palestinians maintain that the Intifada was a protest of Israel's brutal repression which included extra-judicial killings, mass detentions, indiscriminate torture, and deportations; their ultimate goal was to free the occupied territories from Israeli control. These initial protests and conflict resulted in an Israeli military crackdown and the stagnation of the Arab economies in the Occupied Territories. The Intifada was the climax of growing tension and violence between the Israelis and the Palestinians. Although violence eased significantly with the gradual establishment of Palestinian self-rule, beginning with the accord between Israel and the PLO, by the time of the signing of the Oslo Accords in 1993, 1,162 Palestinians and 160 Israelis had died.[67]

2. The al-Aqsa Intifada

The Second Intifada, or al-Aqsa Intifada, resulted from the controversial visit by Israeli opposition leader Ariel Sharon to the holy site known as the Temple Mount (to Jews) or the Haram al-Sharif (to Arabs), the site of the al-Aqsa Mosque in Jerusalem on September 28, 2000.[68] The day after Sharon's visit, following Friday prayers, large riots broke out around Old Jerusalem during which several Palestinians were murdered. In the days that followed, demonstrations erupted throughout the West Bank and in the Gaza Strip. The violence quickly escalated, and within the first six days of the Intifada, 61 Palestinians were killed and 2,657 were injured in what Palestinians and others regarded as "indiscriminate and excessive use of force."[69] This new wave of violence marked the Palestinian frustration towards the failed peace process and slow progress in the region since 1993. Once again, the economic situation in the territories deteriorated, and violence continued to flare including a renewal of suicide attacks in Israel by Hamas, the Palestinian Islamic Jihad, and the PLO and Israeli attacks on official Palestinian installations and reoccupation of areas Israeli forces had previously withdrawn from after

[67] http://www.btselem.org/english/Statistics/First_Intifada_Tables.asp.

[68] This site is disputed by Israelis and Palestinians.

[69] http://en.wikipedia.org/wiki/Al-Aqsa_Intifada#Timeline, last accessed on August 28, 2005.

1993. In particular, the al-Aqsa Intifada is marked by the use of guerilla warfare tactics by Palestinians against the stronger, well equipped and trained Israeli Defense Force.

On February 8, 2005, at the Sharm el-Sheikh Summit of 2005, Israeli Prime Minister Ariel Sharon and Palestinian Authority President Mahmoud Abbas declared a mutual truce between Israel and the Palestinian National Authority. They shook hands at a four-way summit, which also included Jordan and Egypt, at Sharm al-Sheikh; however, Hamas and the Palestinian Islamic Jihad said the truce was not binding for their members. A major shift occurred on February 13, 2005, as Abbas entered talks with the leaders of the Palestinian Islamic Jihad and Hamas, for them to rally behind him and respect the truce. Ismail Haniyah, a senior leader of Hamas, said that "its position regarding calm will continue unchanged and Israel will bear responsibility for any new violation or aggression." May and June 2005 saw a sharp increase in Palestinian terror attacks. In Nablus and Jenin, many Palestinian youth were caught carrying explosives, either as suicide bombers or as couriers. In the Gaza Strip, Palestinian factions such as Hamas, the Palestinian Islamic Jihad, and Popular Resistance Committees carried out daily attacks against IDF outposts and Israeli settlements.[70] These attacks were too much for the Israeli restraint policy, and a growing fear that the terror would render the disengagement plan impossible resulted in Israel resuming its "targeted killing" policy on July 15, 2005. As a result, 7 Hamas militants were killed and about 4 Hamas facilities were bombed. The continuation of shelling rockets over Israeli settlements and fatal street battles between Hamas militants and Palestinian policemen continued to threaten the truce agreed on at Sharm el-Sheikh Summit of 2005. Most recently, conflicts in the region have revolved around Israel's evacuation of settlements in the Gaza Strip and the West Bank.

3. The Palestinian-Israeli Cyberconflict

In addition to the use of Molotov cocktails, suicide bombings, rubber bullets, and targeted killings, the al-Aqsa Intifada has been marked by an intense cyberwar pitting Israeli and Palestinian hackers against one another. While cyber attacks were not new, many have claimed that the Palestinian-Israeli Cyberconflict represents "the first political

[70] http://en.wikipedia.org/wiki/Al-Aqsa_Intifada#2005, last accessed on August 28, 2005.

conflict in which two sides have fought each other in such an organized way over the Internet."[71] Some computer specialists believe that the Palestinian-Israeli Cyberconflict has been the most sustained, malicious hack campaign ever.

Interest in Israeli government websites increased noticeably after the violence which broke out on September 28, 2000; however, according to sources, the "first shot in the cyberwar" was fired by Israeli teens who sabotaged a website of Hezbollah, the militantly anti-Israel guerrilla movement in Lebanon, with a defacement which placed an Israeli flag, Hebrew text, and a recording of "Hatikva" on the homepage. In retaliation, according to Uri Noy, who oversees Israel's Foreign Ministry's website, several extremist Islamic websites called on their users to attack Israeli sites using computer programs that automate attacks by flooding sites with e-mail sent through a Web link. Attacks were carried out against the official site of the Israeli prime minister's office, which was downed; the Foreign Ministry's website, which was overwhelmed by incoming mail and knocked off the Web; the Israeli Defense Force, which repaired its information websites, increased security, and contracted out services to AT&T. Hackers broke into the website of the Knesset and tampered with files. Even Israel's right-wing Likud Party's website was bombarded by several thousand e-mails with messages, such as "Death to the Jews," "Hell is waiting for you," and various obscenities, to mention a few incidents.[72] Similar Israeli websites offered surfers numerous targets, including the sites of Hezbollah, the Palestinian National Authority, and the Palestinian militant group Hamas. One such site, which made it easy for novice users to join in the action, stated "Come and help us stop their pan-Arabic campaign of incitement. Our purpose is not to allow the cruel terror organizations to continue with their sites spreading terror, articles, and sick pictures throughout the Internet." The site then invited users to click on the target they would like to disable, and offered a set of simple instructions for executing assaults.[73] In November 2000, the Arab hackers of UNITY began Phase Three of their

[71] Brian Whitaker, "War Games on the Net: But This Time It's For Real," *The Guardian*, Guardian Unlimited Online, November 30, 2000, last accessed on May 24, 2005.

[72] Lee Hockstader, "Pings and E-Arrows Fly in Mideast Cyber-War," *Washington Post Foreign Service*, p. A01, October 27, 2000.

[73] Lee Hockstader, "Pings and E-Arrows Fly in Mideast Cyber-War," *Washington Post Foreign Service*, p. A01, October 27, 2000.

attacks in an attempt to divert Israeli funds from buying weapons and ammunition to fight the Palestinians by forcing the Jewish state to invest in repairing and safeguarding Internet service providers in Tel Aviv. As evidence that UNITY achieved their goal (at least in part), Alan Abbey, the managing editor of an Israeli website, israel.internet.com, posted an article in which he described how moving hosts out of Israel was shaking up the high-tech business community. According to Israeli Internet Underground, the destruction of business sites with e-commerce capabilities, which they believe caused an 8 percent dip in the Israeli stock exchange, was evidence of Phase Four attacks being carried out by pro-Palestinian attackers against Israel. To further illustrate the serious nature of the Palestinian-Israeli Cyberconflict, according to Jerome Hauer, Internet expert and director of the Crises & Consequences Management Group of Kroll Associates, "the Palestinians have attempted to hack into Israel's air traffic control system in an effort to shut down airports and electronically break into some of Israel's largest companies."[74] The effects of such a successful hack indicate the level to which computer network systems and the Internet can be utilized to affect chaos and disorder, and mass casualties.

Thousands of Israeli and Arab youth joined highly specialized hackers in an attempt to wreak havoc on one another's sites, including sending each other racist, lewd, and occasionally pornographic e-mails, and within their own efforts, circulating website addresses with simple instructions on how to ping, zap, and crash the "enemy's electronic fortresses."[75] The impact of the range of attacks affected not only those sites being targeted, but also other sites and services which relied on the same connections and bandwidth to access the Internet. NetVision, one of Israel's largest Internet providers, published a statement on October 26, 2000 indicating that these overload disruptions to services were caused by an overload by hostile elements trying to compromise government and IDF websites stored on NetVision's servers. According to iDEFENSE Director of Intelligence Production, Ben Venzke, "A shutdown of NetVision would be

[74] Elliot Markowitz, "The New World of Terrorism," *TechTV News*, ZDTV LLC, 2001 http://www.techtv.com/print/story/0,23102,3314752,00.html.

[75] Lee Hockstader, "Pings and E-Arrows Fly in Mideast Cyber-War," *Washington Post Foreign Service*, p. A01, October 27, 2000.

tantamount to knocking Israel off the Net for a significant period of time."[76] Additionally, high profile websites found themselves targeted simply because pro-Palestinian and/or pro-Israeli attackers considered them a good vehicle to promote their cause. Such attacks include those on the American Israel Public Affairs Committee, various Iranian websites to include the Iranian Ministry of Agriculture, various academic institutions, and calls for attacks against high profile corporations such as AT&T and New Jersey-based Lucent Technologies.

As one of the most computer literate societies in the world, Israel should have had an immense advantage in the Palestinian-Israeli Cyberconflict. As of September 2000, when the attacks began, Israel hosted approximately 1.1 million Internet hookups within the Jewish state, more than those in all 22 Arab countries combined.[77] However, Israel's exceptional connectedness offered more targets, making it more vulnerable to attacks. According to Aftahat Ma'Khevim, the branch of military intelligence responsible for computer security, most of the attacks against Israel have been traced to Lebanon and Gulf states, which have the highest number of Internet portals in the Arab world; additionally, many attacks also come from Muslim students at U.S. universities.[78] While the conflicts between Palestinians and Israelis continues, and the Internet continues to play a role in waging attacks against one another, the majority of what has been considered the Palestinian-Israeli Cyberconflict can be encompassed by a series of defacements, denial-of-service attacks, Internet fraud, and attempted cyberterror attacks spanning a few months in the end of 2000. Below, the author provides a thorough analysis of the actors, targets, incidents, and timeline of the Palestinian-Israeli Cyberconflict which ensued between September and December 2000.

[76] Carme J. Gentile, "Hacker War Rages in Holy Land," located at http://www.wired.com/news/politics/0,1283,40030,00.html, November 8, 2000, last accessed on May 24, 2005.

[77] As off April 2002, Israel hosted 2.4 million Internet connections.

[78] "Who's Winning the Arab-Israeli Cyber War?," distributed by Middle East News Online (MiddleEastWire.com), Middle East Intelligence Bulletin, November 15, 2000.

B. PRO-ISRAEL

1. Pro-Israeli Actors

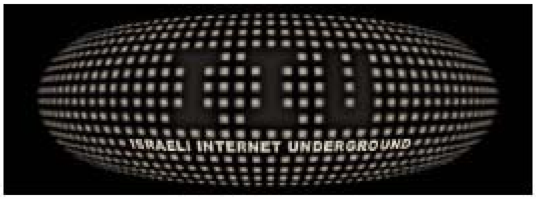
Various individuals and groups, both experienced hackers and average computer users, entered the Palestinian-Israeli Cyberconflict in support of the state of Israel. Whether residents of the state of Israel or individuals working in conjunction with pro-Israeli supporters around the world, these actors utilized the Internet to disrupt, degrade, deny, and destroy the use of the Internet by various pro-Palestinian actors. Additionally, pro-Israeli actors utilized the Internet to spread their message, gain support for their efforts, and offer computer support and security tools to the Israeli government, military, business and public sectors.

The following provides examples of known pro-Israeli actors and actions they carried out during the Palestinian-Israeli Cyberconflict:

- **digibrain & haboshnik**: On October 16, 2000, these actors posted the message, "we are working on a softwhear that will give you control on the hizzballa's ftp with out a password. FUCK HIZZBALLA!!! Sincerely digibrain & haboshanik (we are the domain masters)."
- **Hackers of Israel Unite**: Hackers of Israel Unite is believed to be a group which formed in response to pro-Palestinian attacks against Israeli sites. On November 6, 2000, the group stated on its Web site, "Ok all my israely hackers We are now becoming an army Of the israely Soldiers on the net Our Troopers Canot Die Just Their Computers can burn! Or a site is going to srash! We Are the Israely Soldiers of The internet Our goal is to search and destoy All Of the Arab's Sites on the net! Or to Del as many of the arabs Computers to Kill their Chats and icq's. I need help on the web…So if you dcan send me javas Source I need a java That Does A ping! AnyOne that can help will become a member AnyOne that wants Can Become a Soldier we don't have test but you need tools to fight! All you need to have is a computer and a shell and revenge! (or a fast modem at home.)" The group called for attacks against www.pna.gov.ps, www.almanar.com.lb, www.sis.gov.ps, www.irna.com, and www.albawaba.com. Hackers of Israel Unite is credited with being the first

group on either side of the conflict to call for attacks against chat rooms and ICQ.[79] Around November 12, 2000, the group began distributing WinSmurf through its www.israelhackers.clb.net site.[80] The group claims it was successfully able to down one Arab site with WinSmurf using only a 56K dial-up connection and an ADSL line.

- **Hizballa – No More**: This actor runs an Israeli attack site which advocates ping flood attacks against Hezbollah, Hamas, and other pro-Palestinian sites.
- **Israeli Internet Underground (IIU)**: Formed by a group of “white hat” hackers in response to attacks carried out by pro-Palestinian attackers, IIU works to identify vulnerabilities in Israeli sites and secures them through its SODA project in conjunction with Israeli computer security company 2XS. The stated goal of the project is “to inform and provide solutions wherever we can and therefore protect our sites against political cyber vandalism.”



- **israforce**: An Israeli attack site which advocates ping flood attacks against Hezbollah, Hamas, and other pro-Palestinian sites.
- **lion&type_ohak’eil**: On November 4, 2000, lion&type_ohak’eil defaced the site of the Iranian Ministry of Agriculture, at www.mao.or.ir, in support of the Israelis. lion&type_o ha k’eil threatenened to take down .ir and .lb sites and then .pk sites if Gforce Pakistan continued their defacing of .il sites.
- **Mike Buzaglo**: A then 21-year old Israeli who took credit for the first attacks during the Interfada. In an interview with Israeli television, Buzaglo

[79] ICQ is a real-time chat program created by Mirabilis Ltd. for Windows 95.

[80] WinSmurf is a popular tool which enables one to conduct mass pinging.

claimed he sabotaged the Hezbollah site. He, along with friends, broke into the site and replaced its content with the Israeli flag and the Star of David. Buzaglo is quoted as saying, “We, the Israeli hackers, need to show the right pictures and we will not give a chance, for example, to a Hezbollah site that will show propaganda against Israel. So this is the reason why I decided to attack a couple of Hezbollah sites,” during an interview with CNN. On November 3, 2000, Buzaglo stated that he had ceased launching attacks against anti-Israeli sites, but that he would continue his efforts via his personal site.

- **m0sad:** On Dec. 3, 2000, m0sad defaced the Ministry of Awqaf and Islamic Affairs, Qatar site at http://www.islam.gov.qa in support of the Israelis. m0sad wrote in the defacement, “Now only information has real cost. And it cannot be guarded by armed squad or even by the government special forces. One man can destroy an whole company with one click. Remember about it...”

- **Nir M**: Nir M has claimed defacing the al-Manar site on October 29, 2000.

- **Polo0**: Polo0 has been credited with posting the following on the Internet: several Palestinian officials’ cell phone numbers and instructions on how to access Palestinian fax machines, telephone systems, 24 web sites, 15 Internet Relay Chat (IRC) channels, and the IRC server.

- **Wizel.com**: Wizel.com was utilized by pro-Israeli supporters to host a FloodNet class attack tool, beginning on Oct. 6, 2000. The site’s main logo stated, “ATTACK & DESTROY HiZBALLAH.” The site contained pages both in English and Hebrew. Wizel.com initially targeted six Hezbollah sites, Hamas.org, the Palestinian National Authority at pna.org, Palestine-info.net and Moqawama.org through a FloodNet type tool. The site was hosted by host4u.net in the US, and claimed to have received 21,800 visitors between Oct. 6 and Oct. 24, 2000. The site eventually crashed due to pro-Palestinian counterattacks.

2. Pro-Israeli Sites Hosting Live Attack Tools

Throughout the conflict, individuals and groups established various websites which offered free tools and instructions; and suggested organizations, actors, and sites to target as part of the effort to disrupt, deny, degrade, and destroy pro-Palestinian websites and the operations of pro-Palestinian supporters. Such sites invited users to click on targets they would like to disable, and offered a set of simple instructions for executing assaults against intended targets. The use of pro-Israeli sites hosting live attack tools proved to be the chief means by which Israelis launched attacks against pro-Palestinian actors. Appendix B provides examples of known pro-Israeli websites which hosted live attack tools to be used in CNO against pro-Palestinian actors.

3. Pro-Israeli Targets

Pro-Israeli actors are known to have targeted various pro-Palestinian sites, to include media outlets, Palestinian organizations, governments of foreign states credited with supporting Palestinian terrorist organizations and the Palestinian cause, and the governing body of the Palestinian people. Appendix C provides examples of known sites which were targeted by pro-Israeli actors.

C. PRO-PALESTINE

1. Pro-Palestinian Actors

Individuals and groups throughout the world joined the pro-Palestinian effort during the Palestinian-Israeli Cyberconflict. Known attacks are believed to have originated in areas such as Pakistan, Saudi Arabia, Lebanon, Europe, the United States, and South America. Through various means, pro-Palestinian actors were able to deface pro-Israeli websites, degrade service to Israeli Internet users, disrupt transmission of information and communication, deny Israeli ISPs the ability to provide service, and gather personal data, to include: e-mail addresses, phone numbers, and credit card numbers of Israeli supporters. Additionally, pro-Palestinian actors successfully hacked into official Israeli websites, potentially uncovering and tampering with classified information. Attacks on e-commerce, to include the Tel Aviv Stock exchange, are attributed with causing an 8 percent drop in the Israeli stock exchange and increased security fears amongst businesses and the Israeli populace. Such fears culminated in

Internet users seeking security and Internet service from international providers. Pro-Palestinian actors successfully utilized the Internet to spread their message, recruit members to their organizations, gain global support, finance their efforts, and inhibit the Israeli effort.

The following provides examples of pro-Palestinian actors and actions they carried out during the Palestinian-Israeli Cyberconflict:

- **al-Mujahiroun**: As of January 2001, located at http://www.almuhajiroun.com, al-Mujahiroun was a Muslim extremist group headquartered in London. The leader of al-Muhajiroun in the U.K. was Anjem Choudary. The group had chapters in Pakistan, the U.S., and various countries around the world. The group has been tied to a number of Muslim terrorist organizations and has contact with Osama bin Laden. The group hosted a conference in 1998 in which Hamas, Hezbollah, and Egyptian and Algerian fundamentalist groups took part; and, al-Mujahiroun continues to be a major player in terms of trying to unify the "jihad" campaign against the U.S. and Israel. The group has espoused its belief that the U.S., Israel, Russia, and Britain have declared war on Islam. The British Charity Commission reportedly withdrew al-Muhajiroun's charity license around November of 1999, and the licenses for the Sharia Court of the U.K. and the London School of Sharia were also revoked. These three organizations are supervised by Sheikh Omar Bakri Mohammed, a key figure in al-Mujahiroun. Commenting on the loss of the licenses Sheikh Omar Bakri Mohammed said, "the withdrawal of the Sharia Court's license is part of the attempt to tighten the noose on Islamists in Britain." He added that "in the past, we used to work within the legal limits, but it seems that from now on we have no other option but to work outside the allowed limits." The following message was issued to the members of al-Muhajiroun on there site, http://www.almuhajiroun.com, "We urge you to participate in Phase II of the counterattack against Israeli sites attacking the Moqawama (Islamic Resistance) sites. Enter these web pages and press 'defend the resistance'. A file will start attacking the Israeli Websites as long as you are connected to the net. Open as much windows as you can. http://members.tripod.com/irsa2001, http://www.angelfire.com/oh4/irsa2000, http://irsa2000.jumpfun.com.”

- **Arab Hax0rs**: In a message posted to the Arab Hackers Organization bulletin board on Oct. 22, 2000, Arab Hax0rs claimed responsibility for downing the site at www.gilo.jlm.k12.il. As of January 2001, when iDEFENSE Intelligence Services published its Report on the Israeli-Palestinian Cyber Conflict, it was unclear whether or not Arab Hax0rs is an individual or group.
- **Boss**: On Nov. 8, 2000, with associates tR|cky and KUCAU, Boss defaced www.order-click.co.il and www.dilim.co.il in support of the Palestinians.
- **Brakeoff**: On December 19, 2000, BrakeOff began defacing sites in support of the Palestinians. BrakeOff is a member of the World’s Fantabulous Defacers (WFD).
- **core Hackers (cH)**: The members of cH include tR|cky and xoid. tR|cky is known to have carried out a number of defacements in support of Palestinians.
- **[^CyBeRpUnK^]**: On Dec. 2, 2000, [^CyBeRpUnK^] defaced the Hebrew University of Jerusalem, Israel Web site, at http://shemesh.fiz.huji.ac.il, and the www.as.huji.ac.il site with a pro-peace message. Since then, [^CyBeRpUnK^], a member of the WFD, has begun to deface sites with pro-Palestinian messages. The change in [^CyBeRpUnK^]’s messages began to shortly after m0r0n and nightman joined the WFD.
- **DevilSoul**: DevilSoul, whose members include NiTR8, is suspected of entering the conflict on the pro-Palestinian side on Nov. 12, 2000. NiTR8 defaced two Iranian sites on its first day of activity. It remains unclear why the Iranian sites were targeted as opposed to more traditional pro-Palestinian targets.

- **Doctor Nuker**: Doctor Nuker, who is a member of the Pakistan Hackerz Club (PHC), is credited with infiltrating the American Israel Public Affairs Committee site, at www.aipac.org, on November 2, 2000. During his attack, Doctor Nuker posted pro-Palestinian messages in addition to stealing, and consequently publishing, the credit card numbers and contact information of those who purchased items through the site, member contact information, and thousands of email addresses of individuals who signed up to receive email alerts from the committee. On the defaced site Doctor Nuker said, "This is to inform you that the www.aipac.org web site server is hacked…the web site defaced and all of their users database is compromised. Yes, that includes not only users personal information but their credit card numbers too (that implies to people who have subscribed to their services)… I've put all the email addresses in a file so that you can have an nice mailing list of 3500+ people… The hack is to protest against the attrocities in Palestine by the barbarian Israeli soldiers and their constant support by the US government."
- **dodi**: As of January 2001, dodi had claimed responsibility for defacing three sites and has threatened to take down NetVision's entire network. In his defacement of the Ebrick Inc. Web site, at http://lotus.ebrick.com, dodi wrote, "The time is Sat Oct 21 20:04:22 2000 all of Israel NetVision backbone is offline as of this minute. For those of you who don't know NetVision is the largest internet provider is israel and is host to most of Israels government/comercial networks. NetVision is also the largest public isp in israel and has many dialup access pads and even an dsl network. I think my point is clear... if an islamic site is attacked I down/drop all of israel :)." dodi's first defacement occurred October 12, 2000 when he defaced the Israeli Academic Sub-Domain, at www.netanya.ac.il. On October 20, 2000, dodi proceeded to deface www.jmjservices.com, www.watersportsworld.com, and lab.cvdds.com with the same anti-Israeli message. On November 3, 2000, in a Web page defacement of the COGNIFIT site at www.cognifit.co.il, pro-Palestinian hacker dodi recommended that all wanting to carry out attacks against Israeli sites launch

SYN flood attacks using the “juno” or “slice“ SYN flooder tools against two Domain Name System (DNS) servers run by the NetVision ISP. dodi wrote, “For people wanting a method to easily disable jewish government web pages try hitting dns.netvision.net.il & nypop.elron.net on port 53 with a SYN flooder (I recommend juno or slice) 300 k/sec on each port should see both boxes offline. Doing this ensures no one can resolve any web sites these two nameservers are authoritative to unless they are already cached of course.” An attack of this type against NetVision, which reportedly hosts 70 percent of all the web sites in Israel, could have serious consequences on sites in the region. dodi also wrote, “this isn’t just a war against ‘israel’ for the perpatrators of the attrocities in palestine are US backed. Its America which has blood on its hands the blood of innocent women and children.”

- **EDGE**: EDGE, who is associated with KARTOOS.AK.47, began defacing sites in support of the Palestinians on December 21, 2000. In December 2000, EDGE and KARTOOS.AK.47 formed a group called THE SCYTHE. These two actors are known to have hit sites in both Germany and Japan.

- **Kala**: On October 30, 2000, Kala, claiming to be from Hungary, defaced the Netanya Academic College site, at mars.netanya.ac.il, in support of the Palestinians.

- **KARTOOS.AK.47**: KARTOOS.Ak.47, who is associated with EDGE, began defacing sites in support of the Palestinians on December 21, 2000. In December 2000, EDGE and KARTOOS.AK.47 formed a group called THE SCYTHE. These two actors are known to have hit sites in both Germany and Japan.

- **Kr4kr0k Industries**: On Dec. 20, 2000, Kr4kr0k Industries defaced Arttalk.com, at http://www.arttalk.com, in support of the Palestinians. In their defacement, they stated "The situation in the middle east has gone on for long enough. Palestinians are dying at Israeli hands and the world just lets the whole thing go in one in ear and out the other. Jews are not Gods holy people, nor are they special. What gives them any right to take an innocents life anymore than the next guy. Nothing! That is why Israel needs to stop now. The stage has been set for many years now for the Israelis to have a peacefull resolution, and they have answered yet again with bullets, explosives, and hate. Is this really a holy people? I don't think so. Nuff said." The group also said in the defacement, "security and html provided by antibi0sis."

- **KUCAU**: In association with tR|cky and Boss, KUCAU defaced www.order-click.co.il and www.dilim.co.il in support of the Palestinians on November 8, 2000.

- **GForce Pakistan**: Located at www9.50megs.com/gforce/mirror.htm, GForce Pakistan’s known members include: sniper, heataz, Rsnake, instinct, miller, rave, and nicks xtremist. On November 3, 2000, Pakistani hacker group GForce Pakistan joined the Interfada on the side of the Palestinians. It began defacing Israeli sites: “GForce Declares a War against Israel?…. Ok, GForce Pakistan is back. We really planned not to come back to the defacing scene again, but once again our Muslim brothers needed us.” GForce Paskistan’s involvement in the internet conflict likely increased the number of web page defacements as well as contributed to other attack efforts. On November 4, 2000, the group defaced the sites of Jen Communications, at www.jen.co.il, Health Infosystems Association Israel, at www.healthinfonet.co.il, Visiting Israel Students Association, at www.visa.org.il, Jewish Bible Association, at www.jewishbible.org, and shemayisrael.co.il. The addition of nicks xtremist to the group was announced in the November 8, 2000 defacement of the Ornetix site, at ntserver.ornetix.co.il, and in the defacement of the Radwiz (IL) site, at www.radwiz.co.il. At the same time, GForce Pakistan threatened to launch attacks against DNS servers and NetVision in a defacement of the Terminal-Computers & Multimedia site, at www.terminal.co.il, and a defacement of the Rooster site, at mail.rooster.co.il.

- **Hezbollah**: Hezbollah, or Party of God, was formed in reaction to the Israeli invasion of Lebanon by the IDF in 1982. Many view Hezbollah as a radical Shia group dedicated to the "creation of an Iranian-style Islamic republic in Lebanon and the removal of all non-Islamic influences from the area." Sheik Rafheb was recognized as the leader of Hezbollah until his slaying in 1984. His successor, Sayyid Abbas al-Musawi, led the group in its "liquidation of Israel" until his killing in February 1992. Sheik Hassan Nasrallah, Mussawi's successor expressed, "The only way to achieve a lasting peace in the Middle East is to return all the Jewish occupiers to the lands from which they originally came." Strongly anti-West and anti-Israel, Hezbollah is closely allied with, and often directed by, Iran. Hezbollah has created its own influence within Lebanon, politically, militarily, and socially. Hezbollah is believed to have several thousand members, operating in the Bekaa Valley, the southern suburbs of Beirut, and southern Lebanon. They also have established operations in Europe, Africa, South America, North America, and Asia. Hezbollah receives substantial amounts of financial, training, weapons, political, and organizational aid from Iran and Syria. In recent years, they have used the Internet to successfully advocate their beliefs. Hezbollah's Web site provides detailed information and news on the group's policies and its Web site is widely used for its campaign against Israel. Ali Ayoub, Hezbollah's webmaster stated, "We will never give up the Internet." On October 7, 2000, Hezbollah stated that its web site, at www.hizbollah.org and www.hizballah.org, crashed after allegedly receiving millions of hits from Israel and the US. Ayoub, stated "We have names of 8,521 servers mainly in these two countries that have been hitting our Web site regularly and sending us simultaneously tens of thousands of hostile emails, some of them carrying viruses to sabotage our server." In addition, pro-Israel individuals have allegedly set up several decoy sites, attempting to take advantage of misspellings. One site, www.hizballa.org, contains an Israeli flag with the word "WAR" displayed in flames above, while pro-Israeli music played in the background. In addition, hizballa.com read, “The Official Site of The God’s Party, We are sorry to say Israel was write. The land of Israel belongs to the people of Israel.”

- **Iron Guards**: Iron Guards is a group organized and recruited for by UNITY. Iron Guards began its first announced action during early November 2000. Iron Guards was the result of an organized recruiting campaign by UNITY for skilled hackers and crackers. It is known to be involved in more technically sophisticated attacks that may or may not follow the publicly announced cyber attack plan published by UNITY.
- **Kuds**: Kuds is the distributor of HTTP Bomber 1.0 and HTTP Bomber 1.001b. The kuds.8k.com site was taken down, and the main page was relocated to kuds.8m.com; however, the group continued to utilize the admin@kuds.8k.com email address. The kuds.8k.com site was taken offline sometime on or before November 7, 2000, while iDEFENSE confirmed the “live” status of the kuds.8m.com site on November 7, 2000; however, as of late December 2000, the kuds.8m.com site was down. It is not clear where or if the group relocated site again.
- **lovenectar**: lovenectar, located at http://www.fightisrael.com, runs the attack site, FightIsrael.com. This site served as a distribution point for EvilPing, WinSmurf, and HTTP Bomber 1.01.
- **m0r0n:** In association with nightman, on October 31, 2000, m0r0n defaced two MBA International School of Business Administration Management sites, at www.eiba.biu.ac.il and www.mba.biu.ac.il, in support of the Palestinians. On November 2, 2000, m0r0n and nightman defaced the Shenkar College site, at www.shenkar.ac.il. On November 3, 2000, m0r0n and nightman defaced the site of the Yizrael Valley College (Mihlelet Emek Yizrael), at www.yvc.ac.il, and Israeli Academic site, at www.yvc.ac.il. On November 4, 2000, m0r0n and nightman defaced the sites of www.bayan.co.il, and www.caspit.co.il. On December 1, 2000, m0r0n and nightman defaced the site of the SOMA Gallery in Northport, NY, at http://www.somagalleries.com. This defacement marked an announcement that m0r0n and nightman were joining with the “World's

fantabulous defacers" (WFD), and included Macromedia Flash animation, stating: "we will be defacing for them because they are helping us spread the word. Anyone interested in helping us spreading the word is most welcome." On December 27, 2000, m0r0n, nightman, and fighter4Isl@m announced the beginning of Phase 5 of the pro-Palestinian side in a defacement of the www.order-click.co.il site. The message read, "Note to All Pro-Palestinian Hackers Involved in the Cyber-War: Just a few weeks ago, you will recall that Unity was leading this war. Unity's voice apparently was silenced by the Zionists and their supporters and their site as a result was taken down. Their needs to be unity among us, for we are indeed one brotherhood, and whether we are Pakistani, Arab, African, Brazilian, or any other nationality, we are fighting for the one and the same purpose. Their needs to be a leader in this fight, and we are going to try to take a leading role in this war. Phase 4 by Unity was originally planned to cause Israeli companies and organizations immense economic losses. Whether or not this phase actually went forward or not, we need to move on with Phase 5. Phase 5 'Global Awareness' involves exactly what the name implies, awarness in every sector and realm of the Internet about the truth about what is occuring in Palestine. After an anonymous Israeli hacker defaced Hizballah on December 26, we decided to move forward with this phase. Global Awareness constitutes everything from email bombs to message board postings to defacements. Defacement is the weapon of choice. Email us at wfd2000@hushmail.com at tell us what you feel about it. The cyberwar has not ended. It has just begun. The cyberwar will never end as long as the furious, unforgiving rockets, bullets, and missiles of Zionism fire upon the innocent Muslim and Christian children of Palestine.

Signed,

- World's Fantabalous Defacers

P.S. - Phase 5 'Global Awareness' has now been initiated. Please note that Phase 5 is planned to be a very benevolent phase, so you geezers at IDEFENSE don't need to feel the urgency to monitor our every move. Our policy is not to destroy, but to deface. Oh yes, and if Hizballah's website is attacked again in anyway, it will be met immediately with swift retribution.

TO ADMIN: Your database has remained unharmed and untouched as have those of all our other 'victims', but if we are provoked by you or your ally organizations in any way, matter, shape, or form, we will certainly not hesitate to go beyond defacements, because we certainly have the ability to."

An additional defacement stated, "You have been hacked by m0r0n and nightman of Pakistan and there is only one reason behind this defacement and that is the WAR OF ISRAEL with PALESTINIANS! Stop the violence and STOP killing Muslims (that includes children and women!). There is no need for us to delineate the nature of Israel and their CORRUPT POLITICIANS because we all known about their pervert nature! What we want to show here is not that server is vulnerable but through this hack we want to create AWARENESS amongst the people of how non-human Israel can be. Violence never leads to victory, WAR LEADS TO A DEAD END!!! A very simple example is alos of KASHMIR and the war of the MUJAHIDEENS (Freedom fighters) againstIndia! SO the conclusion here is TOP VIOLENCE IN PALESTINE AND KASHMIR! Greetz to GFORCE Pakistan, DoctorNuker, Anti Security, Aniclator, and all those who support us by their heart rending emails of which we are planning to quote a few of them in our upcoming HACKS! All queries to m0r0n@cheerful.com and nightman@husmail.com. Peace@KAHMIR and PEACE@Palestine. LONG LIVE PAKISTAN."

- **Murtaza Baloch (a.K.a. EdGe)**: On November 15, 2000, Murtaza Baloch (a.k.a. EdGe) defaced the www.karate.org.il site in support of the Palestinians. It remains unconfirmed whether or not this is the same EDGE that has been associated with KARTOOS.AK.47.

nightman: On October 31, 2000, in association with m0r0n, nightman defaced two MBA International School of Business Administration Management sites, at www.eiba.biu.ac.il and www.mba.biu.ac.il, in support of the Palestinians. On November 2, m0r0n and nightman defaced the Shenkar College site, at www.shenkar.ac.il. On November 3, 2000, m0r0n and nightman defaced the site of the Yizrael Valley College (Mihlelet Emek Yizrael), at www.yvc.ac.il, and Israeli Academic site, at www.yvc.ac.il. On November 4, 2000, m0r0n and nightman defaced the site of www.bayan.co.il and www.caspit.co.il. On December 1, 2000, m0r0n and nightman defaced the site of the SOMA Gallery in Northport, NY, at http://www.somagalleries.com. The defacement marked an announcement that m0r0n and nightman were joining with the "World's fantabulous defacers" (WFD), and the hack, which included Macromedia Flash animation, stated: "we will be defacing for them because they are helping us spread the word. Anyone interested in helping us spreading the word is most welcome." On December 27, 2000, in a defacement of the www.order-click.co.il site, m0r0n, nightman, and fighter4Isl@m announced the beginning of Phase 5 in support of the Palestinian side.[81]

- **Pakistan Hackerz Club (PHC)**: The Pakistan Hackerz Club, whose members include Doctor Nuker, joined the cyberconflict on the side of the Palestinians on November 2, 2000 with their defacing Israeli sites.

- **ReALiST**: ReALiST claimed responsibility for Web page defacements against egynile.com and cairo.eun.eg/hacked.asp. He is known to be a member of the Xegypt hacker group. In a message posted to an Arab hacker bulletin board, ReALiST wrote, "I'm thinking of something like DDoS, on major Israel networks and sites, and sending emails helping all Arab ISP's and sites for more security, we will just tell them what we know... I'm thinking of installing TFN3K servers and doing the cnn.com and Yahoo.com thing again any one in, mail me quick." ReALiST, along with PROJECTGAMMA, also claimed responsibility for the

[81] To view the messages left in nightman's defacements, see the aforementioned description for m0r0n.

defacement of www.aucegypt.edu/hi.htm, in which the defaced page read, "ReAlist+ProjectGamma Defaced This Sie,Cyber Jihad Has Begun,MicroSoft Was Hacked Why Dont You?" On September 2, 2000, on the bulletin board of the Arab Hackers Association, ReALiST posted a message stating, " salam y'all its really an annoying matter when i ever think of it,all the IT Rise all over the world and we are now sure electronic WAR wont be underestimated , so will there ever be arab cyber warriors to attack,defend..when it is really needed. when i see arab cyber users ,I only see Chatting,MP3's,Pornography and other trivial stuff,And Tim Is So Critical in that case,i myself will never save any piece of info or help for any wannabe or beginner,and thats what every one do... thx"

- **tR|cky**: tR|cky, a member of core Hackers (cH), is known to be associated with Boss, KUCAU, petite_lourve, and xoid. On November 8, 2000, tR|cky, Boss and KUCAU defaced www.order-click.co.il and www.dilim.co.il in support of the Palestinians. On November 18, tR|cky and petite_lourve defaced the Open University-Jerusalem site, at http://online.achva.ac.il.
- **Ummah.net**: Named for the "community of believers," Ummah.net is a Web hosting and Islamic Gateway based in the U.K. The company hosts the Web sites for the Muslim Hackers Club (MHC), the MHC's Houston Chapter, UNITY and other Muslim extremist sites. The site was also once home to the web pages of al-Muhajiroun and Supporters of Sharia.
- **UNITY**: UNITY, a Muslim extremist group with ties to Hezbollah and other terrorist organizations, began "Phase 3 of its Cyber War" on October 31, 2000. Phase 3 targeted the Israeli ISP infrastructure through the use of the "defend" tool (Phase 3 release) and through other more sophisticated methods. Initial targets included www.lucent.com, www.webstyle2000.com, www.goldenlines.co.il, and www.comsec.co.il. Other ISPs or telecommunications companies, either operating in Israel or with a visible business presence in the region, were also at risk. Phase 1 targeted predominately official government sites, while Phase 2 expanded the scope to include such targets as the Tel Aviv Stock Exchange and Bank of Israel. On October 31, 2000,

UNITY announced its intention to launch Phase 4 in the near future, "we warn the Zionist and their supports that any attempt to touch any Anti-Zionist site, will be faced by phase 4 of the cyber war, which will be: 'Attacking Zionist E-Commerce' sites with millions of dollars of losses in transactions." UNITY has been credited with forming the Iron Guards group, which has been active in carrying out more sophisticated cyber attacks against Israeli sites.

- **Unix Security Guards (USG)**: Unix Security Guards, which was formed in May 2002, is a pro-Islamic group which increased its activity tenfold in September 2002 to highlight the Palestinian cause and show solidarity with the Arab world as tensions rose in regard to the U.S. conflict with Iraq. The group consists of five member sub-groups: rD, Inkubus, Egyptian|Fighter, hein, and ShellCode located throughout the Middle East and Eastern Europe. USG's stated aim is "to show the world how our brothers are suffering in Iraq, Palestine, etc and how Israel turned into some cold blooded killing machine[s]." Their attacks included tampering with data on online systems and denial-of-service attacks.
- **Walid**: In the October 26, 2000 edition of the Lebanese Daily Star, Walid is quoted as saying that he intended to hack into the Knesset server late on October 25, 2000. Walid stated, "We'll target and hack Israeli websites one by one. This will continue." He added that the attacks may get fiercer, with an email war between Israel and Arabs including an exchange of viruses designed to crash systems.
- **World's Fantabulous Defacers (WFD)**: WFD joined the cyber side of the conflict around November 20, 2000, defacing with pro-Palestinian and/or anti-war content. On December 1, 2000, with the addition of m0r0n and nightman to the ranks of WFD, this Pro-Palestinian cracker group intensified its cyber campaign. Sources indicate that at least 64 sites were defaced, in varying degrees, since the beginning of the month. All defacements called for "global awareness"

of the Israeli-Palestinian conflict. Some content, especially the defacements conducted by m0r0n and nightman, contained gruesome photographs. Of the 64 sites defaced since the beginning of December, a dozen were U.S. educational institutions including kindergarten through 12th grade schools as well as colleges and universities. Six sites were governmental sites including the federal government and local municipalities. The U.S. Centers for Disease Control site, at http://phil.cdc.gov, was defaced on December 23, 2000 by WFD. Most of the sites defaced, 56 out of 64, were running Windows NT 4.0 with Internet Information Server 4.0. However, WFD defaced four sites running Unix, three servers running Silicon Graphic Inc.'s Irix, and one running IBM Corp.'s AIX. The operating systems of the remaining servers are uncertain. At least 11 people claim membership in WFD. The following provides a breakdown, as of January 2001, of the breakdown for the defacement campaign based on WFD's members:

1. 1B_Real defaced four sites alone, but paired with Brake^Off for two defacements and CyBeRpUnK for one other defacement.

2. b1n4ry c0d3 defaced only one site on December 3, 2000. This defacement was the only one to refer to the WFD as the "World's Fuck Defacers."

3. Brake^Off, by far, was the most active in the defacement campaign, hitting 25 sites. Brake^Off's defacements tended to be text-only. As of January 2001, Brake^Off's email was elbarto224@usa.net.

4. CyBeRpUnK hit five sites alone, but also worked with nightman on two defacements and B_Real on one. As of January 2001, CyBeRpUnK's email address was cyberpunk_2000@hushmail.com.

5. fighter4isl@m is known to have authored the Macromedia Flash content for some of m0r0n and nightman's defacements. On December 26 and 27, 2000, fighter4isl@m was listed as an equal partner with m0r0n and nightman on two defacements.

6/7. As of January 2001, h3ll rais3r always worked with laughing 3y3s, hitting five sites since December 16, 2000.

8. As of January 2001, m0r0n always worked with nightman. Since December 1, 2000, m0r0n and nightman defaced 10 sites under the name of WFD and three sites without any mention of WFD. m0r0n and nightman's defacements became more sophisticated, incorporating Macromedia Flash objects written by fighter4isl@m. Two sites, one defaced on December 26 and the other on December 27, 2000, completely credited fighter4isl@m for the defacements. As of January 2001, the email address for nightman and m0r0n was m0r0nandnightman@hushmail.com.

9. nightman normally worked with m0r0n, completing 10 site defacements; however, nightman executed two defacements with CyBeRpUnK. As of January 2001, the email address for nightman and m0r0n was m0r0nandnightman@hushmail.com.
10. SoFh hacked only one site and used the email address sofh@nightmail.com.
11. Tå|{ê Ñø £Øgîç defaced three sites during the cyber campaign.

Three defacements mentioned WFD, but were unsigned. WFD's attention on U.S. institutions was, and continues to be, cause for concern. Generally, the defacements were not destructive, leaving original content untouched. However, defacements included content from WFD with plans for increasing defacements as 2000 ended and 2001 began. Administrators were urged to assure all web server software had been patched and monitor throughout the holiday period and into 2001.

- **Xegypt**: Xegypt membership includes ReALiST and m0h. While Xegypt itself has not formally claimed any attacks against Israeli sites, group member ReALiST was active in support of the Palestinians. Sometime in October or November, 2000, the group's Web site was forced offline. It is not clear if this was due to the group's involvement with the cyber conflict or other unrelated issues.
- **xoid**: In association with tR|cky, on November 19, 2000, the two defaced the Open University-Jerusalem site, at http://www.jccopenu.ac.il, in support of the Palestinians. xoid is a known member of core Hackers (cH).

2. Pro-Palestinian Sites Hosting Live Attack Tools

Various pro-Palestinian Web sites provided users with instructions and tools to attack Israeli Web sites. Hackers often penetrated Israeli sites and later posted Internet addresses for sympathetic "cyber soldiers" to target with flood attacks to crash Israeli government Web sites. Additionally, Internet chat rooms, popular among Arabs, and bulletin boards were used to circulate information in order to coordinate attacks and instruct participants on how to attack pro-Israeli sites. Pro-Palestinian sites often offered free tools which flooded Israeli sites with thousands of pings, sent thousands of emails to targeted addresses, and assisted in the defacing and degrading of pro-Israeli Web sites.

Appendix D provides examples of known pro-Palestinian Web sites which hosted live attack tools to be used in CNO against pro-Israeli actors.

3. Pro-Palestinian Sites Supporting the Campaign

In addition to pro-Palestinian Web sites which hosted live attack tools, various pro-Palestinian Web Sites directly supported the campaign against Israel. These sites provided suggested sites and organizations to target, offered instructions on how to execute cyber attacks, provided an arena to coordinate actions, and supplied an endless flow of propaganda from which pro-Palestinian actors gained motivation to carry out attacks. Appendix E provides examples of known pro-Palestinian Web sites which supported the campaign against Israel and Israeli supporters.

4. Pro-Palestinian Targets

Pro-Palestinian actors around the world united around the use of the Internet to launch attacks against Israeli official government sites, e-commerce sites, academic institutions, media outlets, and pro-Israeli sites. In an attempt to gain global support for their cause, some pro-Palestinian actors targeted sites with messages describing Israel's atrocities towards Palestinians within the Occupied Territories. Others targeted sites which they believed represented individuals, institutions, and organizations which supported Israel and its oppression of the Palestinian people. The vast majority of pro-Palestinian actors targeted sites which they believed would disrupt Israel's ability to access the Internet, would induce fear amongst Israel's populace, and would draw the most attention to their cause. These targeted sites were often attacked with defacements, which altered the content of their homepages. Additional attacks included third-party sites, which were targeted as a result of their utility to Israel. Appendix F provides examples of known pro-Israeli Web sites which were targeted by pro-Palestinian actors during the Palestinian-Israeli Cyberconflict.

D. OUTSIDE PARTICIPANTS

The Palestinian-Israeli Cyberconflict was not confined to Palestinians and Israelis. Besides those individuals and groups which directly supported one side or the other in this conflict, various actors around the world participated in CNO to target sites with messages of peace. Through Web site defacements, these outside participants informed their audiences of the atrocities taking place in the region as a result of continued tensions between Palestinians and Israelis. All evidence indicates that such defacements were purely non-destructive, and were executed in attempts to deride Palestinians and Israelis for their non-progressive behavior. Additional defacements call on the international community to support a long-term peace effort in the Middle East region. Appendix G provides examples of known outside actors, who participated in attacks, and extraneous websites, which were targeted, during the Palestinian-Israeli Cyberconflict.

E. PALESTINIAN AND ISRAELI CYBER INCIDENTS

Below, the author provides a list and description of the major incidents which took place during the main campaign of the Palestinian-Israeli Cyberconflict. These incidents represent various computer network operations executed by both pro-Palestinian and pro-Israeli actors. Such incidents include examples of websites defacements, cyber espionage, swarming, denial-of-service attacks, and computer virus attacks.

- **al-Manar Site (almanar.com.lb)**: On October 29, 2000, a pro-Israeli attacker, under the name Nir M, defaced Hezbollah's al-Manar site. The attacker uploaded an animated Israeli flag to the site, a link to information about Palestinian rioters, and photographs of the lynching of two Israeli soldiers in Ramallah.
- **American Israel Public Affairs Committee (www.aipac.org)**: On November 2, 2000, Doctor Nuker broke into the American Israel Public Affairs Committee site (www.aipac.org) and posted pro-Palestinian messages in addition to the credit card numbers and contact information of those who made purchases through the site, member contact information and the email addresses of thousands who signed up to receive email alerts.
- **Bank of Israel**: The Bank of Israel has been under attack by pre-configured FloodNet type tools since at least October 25, 2000.
- **al-Bawaba Portal**: This Arab portal site, based in Jordan, was attacked by pro-Israeli supporters in early October 2000. According to a November 5, 2000 Jerusalem Post report, "The attack, called denial of service… flooded the

portal's political forum chat room with heavy graphics files insulting Islam, the Prophet Mohammed, Yasser Arafat, and the Palestinian Authority, forcing it to shut down. The assault was apparently taking the forum's hot debates one step further, said Ramzy Khoury, Al-Bawaba's editor in chief, who added that the attack was the first in a series; the last of them came this week on the site's e-mail server. The first few attacks have already been traced to an organized Israeli effort to attack the Arab portal, with Web pages posted on Israeli sites automatically starting an assault when opened."

- **Bayan.co.il**: On November 4, 2000, m0r0n and nightman defaced the site of bayan.co.il. In this defacement, the duo continued their attacks against Israeli sites claiming "Anything anti-muslim will be hacked!" "Our motto is simple and clear and that is to CREATE GLOBAL AWARENESS AMONGST the world so that everyone would come to know of the attrocities done to Muslims all round the world. And shouts to DoctorNuker for his hack...too!"
- **Cairo.eun.eg/hacked.asp**: On October 25, 2000, pro-Palestinian hackers ReALiST and PROJECTGAMMA, defaced the site of www.cairo.eun.eg. A message posted to the site stated, "PALESTINE CHILDEREN IN DANGER"
- **COGNIFIT (www.cognifit.co.il)**: dodi defaced www.cognifit.co.il on November 4, 2000. dodi continued to express his pro-Palestinian stance, "this isn't just a war against 'israel' for the perpatrators of the atrocities in palestine are US backed. Its America which has blood on its hands the blood of innocent women and children." dodi further defaced the site with the banner "Jihad, Islmic Unity," as well as the warning to the IDF: "I don't care where you move your propaganda machine, I will continue to take it out." In this defacement, dodi recommended that all wanting to carry out attacks against Israeli sites should launch SYN flood attacks using the "juno " or "slice" SYN flooder tools against two Domain Name System (DNS) servers run by the NetVision ISP.
- **www.caspit.co.il**: On November 4, 2000, m0r0n and nightman defaced the Automated Transaction System, at www.caspit.co.il, in support of the Palestinians. The two stated, "You have been hacked by m0r0n and nightman of

Pakistan and there is only one reason behind this defacement and that is the WAR OF ISRAEL with PALESTINIANS! Stop the violence and STOP killing Muslims (that includes children and women!)." The two also expressed "Greetz to GFORCE Pakistan,DoctorNuker,Anti Security, Aniclator and all those who support us by their heart rending emails of which we are planning to quote a few of them in our upcoming HACKS!"

- **Ebrick Inc.**: On October 21, 2000, pro-Palestinian attacker dodi defaced the lotus.ebrick.com site of Ebrick.
- **Health Infosystems Association, Israel (www.healthinfonet.co.il)**: On November 3, 2000, GForce Pakistan defaced the site of Health Infosystems Association, Israel in support of the Palestinians.
- **Gega Net ISP**: Gega Net is a branch of the Egyptian German Telecommunications Industries (EGTI) and is one of the most popular ISPs in Egypt. PROJECTGAMMA claimed responsibility for the defacement.
- **Gilo.jlm.k12.il**: The site of a high school in Jerusalem hosted by NetVision. PROJECTGAMMA claimed responsibility for attacking the site.
- **Hamas.org**
- **Hezbollah Site (hezbollah.com, 207.222.197.194, 216.147.45.137)**: After being targeted by millions of hits and hostile emails from Israel and the United States, Lebanon's Hezbollah guerrilla group said its Web site crashed on October 7, 2000, the day Hezbollah guerrillas captured three Israeli soldiers in an ambush at the border in south Lebanon. Hezbollah webmaster Ali Ayoub said, "We have names of 8,521 servers mainly in these two countries [US and Israel] that have been hitting our Web site regularly and sending us simultaneously tens of thousands of hostile emails, some of them carrying viruses to sabotage our server…This is a well known method used to kill websites. This is Israeli technological warfare." During the week of October 23, 2000, Israelis broke into Hezbollah's server and inserted an Israeli flag and the "Hatikvah" on the Islamic militia's Web site.

- **Inconet**: Inconet is an ISP that hosts a number of the Hezbollah sites. According to Inconet's Mahasen Ajam, the company was targeted by sources that "originated in Israel from five different sites, four of them official. This is a new way of fighting and just like they used to attack our infrastructures with planes, now they might attack our Internet and technological capacities. We have to be ready."

- **Injustice**: On Marcy 20, 2001, the Palestinians sent the first politically motivated mass mailing computer virus, "Injustice." "Injustice," named "Staple" by anti-virus experts, infected global e-mail accounts seeking help for the Palestinian cause. The virus appeared as an attachment to an e-mail message with the subject line "RE: Injustice" and the following message, "Dear (Outlook User name)/ Did you send the attached message, I was not expecting this from you!" While largely benign, rated as a medium threat, the virus sent itself to the first 50 addresses in the recipient's address book, along with 18 Israeli government addresses, 8 Israeli organizations, and to the Webmaster of Israel's official Web site. Finally, "Injustice" used Microsoft's Internet Explorer to open six windows to a variety of Web sites, including an electronic petition to the United Nations High Commissioner for Human Rights."

- **Iranian Ministry of Agriculture**: On November 4, 2000, lion&type_o ha k'eil defaced the site of the Iranian Ministry of Agriculture, at www.moa.or.ir in support of the Israelis. Lion&type_o ha k'eil threatened to take down .ir and .lb sites and then .pk sites if GForce continued defacing .il sites.

- **Israeli Academic (www.yvc.ac.il)**: On November 3, 2000, m0r0n and nightman defaced the Israeli Academic site at www.yvc.ac.il in support of the Palestinians.

- **Israeli Defense Forces (IDF) Site**: According to UNITY, on October 28, 2000, "Although the IDF cooperated with AT&T to provide an advanced security to its web site, the site was disabled for couple of hours last night due to a Cyber attack." The site has been under attack by a number of sites deploying FloodNet type tools since at least October 25, 2000 and possibly earlier. In mid-November, 2000, www.israeldefenseforce.com presented a page almost identical to the real Israeli army spokesperson's site at www.idf.il. The logo was the same, except for a missing letter, and both sites carried photographs of four Israeli soldiers killed by Palestinian gunmen in the West Bank and Gaza Strip. The major difference between the two sites, was the captions and headlines found on the bogus site, which stated "The four Israeli soldiers murdered just before their trip to the West Bank on a mission to kill Palestinian civilians," "We are happy to announce that we killed five babies," and "We have successfully placed smoke and tear gas bombs in all Christian churches and Muslim mosques." It is highly likely that the site has been under additional types of attack as well.

- **Israeli Ministry of Foreign Affairs Site**: Due to attacks, the Israeli Foreign Ministry site went down for more than three days. The site reportedly first went down of October 25, 2000. Computers at the Israeli Ministry of Foreign Affairs crashed due to thousands of "hits" carried out by Palestinians and their sympathizers.

- **Israeli Government (israel.org)**: The site has been under attack by a number of sites deploying FloodNet type tools since at least October 25, 2000 and possibly earlier. It is highly likely that the site has been under additional types of attacks as well.

- **Israeli Knesset Site**: Knesset Spokesman Giora Pordes said attackers broke into the site and tampered with its files. Pordes said the attack may have come from Saudi Arabia.

- **Israeli Prime Minister's Office Site**: The site has been under attack by a number of sites deploying FloodNet type tools since at least October 25, 2000 and possibly earlier. It is highly likely that the site has been under additional types of attacks as well. UNITY issued a statement on October 28, 2000 that said, "After discovering the trick that made the Zionist Prime Minster Office site revive, the site was sent down last night, it is still down till the moments of writing this report (www.pmo.gov.il), and our greetings to the staff of Tehila Security team for their bad job in protecting the main governmental sever in the Zionist entity." During the week of October 23, 2000, suspected pro-Palestinian attackers attempted to overload the servers hosting the Jerusalem Post, which uses NetVision to host its site.

- **Jewish Bible Association (www.jewishbible.org)**: On November 3, 2000, the site of the Jewish Bible Association, at www.jewishbible.org, was defaced by GForce Pakistan in support of the Palestinians.
- **MBA International School of Business Administration Management (www.eiba.biu.ac.il and www.mba.biu.ac.il)**: On October 31, 2000, m0r0n and nightman defaced the MBA International School of Business Administration Management sites, at www.eiba.biu.ac.il and www.mba.biu.ac.il, in support of the Palestinians.
- **Jen Communications (www.jen.co.il)**: On November 3, 2000, Jen Communications' site was defaced by GForce Pakistan in support of the Palestinians.
- **Jerusalem Post**
- **Netanya Academic College (mars.netanya.ac.il)**: On October 30, 2000, Kala defaced the Netanya Academic College site, at mars.netanya.ac.il, in support of the Palestinians.
- **NetVision**: NetVision released a statement on October 26, 2000 saying that it was having difficulty maintaining its services due to the attacks against government sites that it was hosting. NetVision General Manager Gilad Rabinovich said, "We are taking measures, which for obvious reasons, we would rather not reveal, to prevent similar attacks. We have not come across to date any case in which access to the Internet through us was shut down for even a moment." After further questioning by a journalist, Rabinovich said, "NetVision is exposed to serious violence which is part of the struggle between Israel and Palestinian groups. This violence, which consisted of hacker attacks to try to crash official Web sites of the State of Israel, caused blockages to Internet infrastructures and damaged services the company offers it customers."

- **Pf1 Systems Ltd. (www.pf1.co.il)**: On November 3, 2000, the site of Pf1 Systems Ltd. was defaced by GForce Pakistan in support of the Palestinians.
- **Shemayisrael.co.il**: On November 3, 2000, shemayisrael.co.il was defaced by GForce Pakistan in support of the Palestinians.
- **Shenkar College (www.shenkar.ac.il)**: On November 2, 2000, m0r0n and nightman defaced the site of Shenkar College, at www.shenkar.ac.il in support of the Palestinians.
- **Tel Aviv Stock Exchange Site**: The site has been under attack by a number of sites deploying FloodNet type tools since at least October 25, 2000 and possibly earlier. It is likely that the site has been under additional types of attack as well. UNITY issued a statement on October 28, 2000 that said, "Zionist Stock Exchange were disabled last night for 5 hours."
- **Visiting Israel Students Association (www.visa.org.il)**: On November 3, 2000, GForce Pakistan defaced the site of the Visiting Israel Students Association in support of the Palestinians.
- **Yizrael Valley College (Mihlelet Emek Yizrael) (www.yvc.ac.il)**: On November 3, 2000, m0r0n and nightman defaced the site of Yizrael Valley College (Mihlelet Emek Yizrael), at www.yvc.ac.il, in support of the Palestinians.

F. TOOLS USED DURING THE PALESTINIAN-ISRAELI CYBERCONFLICT

Activity by pro-Palestinian and pro-Israeli attackers included FloodNet-type attacks, system penetrations, other more sophisticated attacks, and viruses. Throughout the Palestinian-Israeli Cyberconflict, pro-Palestinian and pro-Israeli actors utilized tools to execute assaults against targeted websites and e-mail addresses. These tools enabled actors to execute ping attacks, HTTP GET requests, Web attacks, and denial-of-service attacks. Through use of these tools, pro-Palestinian and pro-Israeli actors successfully defaced one another's websites, disrupted transmissions, degraded Internet service, exploited Internet websites, tampered with confidential information; and caused millions of dollars in damage, "clean up," and security implementation. Appendix H provides a list of some of the tools used during the Palestinian-Israeli Cyberconflict.

G. TIMELINE OF THE PALESTINIAN-ISRAELI CYBERCONFLICT

The main campaign of the Palestinian-Israeli Cyberconflict took place during a four-month span at the end of 2000. During that time, pro-Palestinian and pro-Israeli actors targeted pro-Israeli and pro-Palestinian websites, organizations, and supporters in an attempt to degrade each other's ability to utilize the Internet, to infiltrate official government/governing body websites, to inflict economic damage, to incite fear amongst the populous, and to gain international support for their cause. Through the use of CNO, pro-Palestinian and pro-Israeli actors successfully infiltrated official government websites, defaced hundreds of websites, inflicted millions of dollars in damage and "clean up," and progressed the computer security industry. The author provides the following timeline to illustrate the events which constitute the main campaign of the Palestinian-Israeli Cyberconflict:

September 27, 2000:

- Palestinian leaders warned of possible danger if Sharon visited holy sites.

September 28, 2000:

- Sharon entered old city.

September 29, 2000:

- Two Web sites of the Lebanese Islamist movement Hezbollah, www. Hizbollah.org and www.hizballah.org, were swamped by e-mail messages, considerably slowing down their processing rate.

October 6, 2000:

- Wizel.com attack tools went online, at http://www.wizel.com.

October 7, 2000:

- The site at http://www.hizbollah.org was hit.

October 12, 2000:

- USS Cole was attacked off the coast of Yemen.
- Two Israeli soldiers were killed in Ramallah.

October 16, 2000:

- Peace summit was held in Egypt.
- U.S. State Department issued warnings.

October 18, 2000:

- Unconfirmed reports suggested that some Israeli systems were hit by cyber attacks.

October 20, 2000:

- Hezbollah webmaster Ali Ayoub verified that its site had been hit.
- JMJ Internet Services, at http://www.jmjservices.com, was defaced by dodi.

October 21, 2000:

- Ebrick Inc., at http://lotus.ebrick.com, was defaced by dodi.
- Arab League opened summit in Cairo.

October 23, 2000:

- Israeli government systems continued to be plagued by cyber attacks.

October 24, 2000:

- Clinton invited Arafat to Washington.

October 25, 2000:

- Wizel.com, at http://www.wizel.com, was listed as possible target by anti-Israeli web site.
- Israeli Government site, at http://www.israel.org, Israeli Defense Forces (IDF), at http://www.idf.il, and Wizel.com, at http://www.wizel.com, were targeted by the pro-Palestinian attack site Ummah.net, at http://www.ummah.net/unity/defend, which hosted the "defend" tool.
- ReALiST, a pro-Palestinian attacker, claimed credit for the defacement of EgyNile Internet service provider site, at http://www.egynile.com.
- ReALiST and ProjectGamma claimed credit for the defacement of Cairo University's site, at http://www.cairo.eun.eg.
- ReALiST, using the name Anti-Israel, posted a message saying, "I'm thinking of something like DDoS, on major Israel networks and sites, and sending emails helping all Arab ISP's and sites for more security, we will just tell them what we know... I'm thinking of installing TFN3K servers and doing the cnn.com and Yahoo.com thing again any one in, mail me quick."
- Computers at the Israeli Ministry of Foreign affairs crashed due to thousands of "hits" carried out by Palestinians and their sympathizers.

October 26, 2000:

- Bank of Israel, at http://www.bankisrael.gov.il, was targeted by pro-Palestinian attack site.
- Israeli Foreign Ministry site, at http://www.mof.gov.il, was forced down by attackers.

- Tel Aviv Stock Exchange site, at http://www.tase.co.il, was targeted by pro-Palestinian attack site.
- Israeli Knesset site was attacked by pro-Palestinian attacker; a Lebanese attacker known as Walid claimed responsibility.
- Islamic extremist group al-Muhajiroun urged individuals to participate in cyber attacks against Israeli web sites, listing the following attack sites: http://members.tripod.com/irsa2001, http://www.angelfire.com/oh4/irsa2000, and http://irsa2000.jumpfun.com.
- NetVision, one of Israel's largest Internet providers, published a statement saying that the partial disruption to services was due to an overload caused by hostile elements trying to shut down government and IDF Web sites stored on NetVision's servers.
- The Israeli army hired AT&T to reinforce its service and protect it from crashing.
- Israel radio stated that "a concerted campaign of jamming" by Islamic groups around the world put several official Israeli sites, including those of the Israeli parliament, the Foreign Ministry, the prime minister's office, and the IDF, out of action.

October 27, 2000:

- Another Hezbollah site, at http://www.hizballah.org, was reported down due to an overwhelming number of hits.
- Pro-Israeli attackers created several decoy sites targeting Hezbollah site visitors; the two decoy sites were located at http://www.hizballa.org and http://www.hizballa.com; both sites contained pro-Israeli messages.
- Israeli Army established contracts with AT&T Corp. to help deal with cyber attacks.
- Messages began circulating among students at universities in the U.S., asking students to contribute to online actions against pro-Palestinian web sites.

October 29, 2000:

- al-Manar Television, a Hezbollah news site at www.almanar.com.lb, was defaced by Nir M. The defacement included the displaying of an Israeli flag, while the home page had a link to another Web site about the lynching of two Israeli soldiers in Ramallah. www.manartv.com, also maintained by Hezbollah, continued to operate normally.

October 30, 2000:

- Israeli Knesset site was restored.
- UNITY issued a call for Muslims and Arabs in the U.S. to boycott AT&T Corp.
- ReALiSt+ProjectGamma claimed credit for defacing the site belonging to The American University in Cairo, at http://www.aucegypt.edu/hi.html.
- UNITY's attack site, at http://www.ummah.net/unity/defend /, was moved to http://defend.unity-new.com/ and http://hizbollah.unity-news.com/ after the ISP

hosting Ummah.net threatened to take its sites offline if the attack site was not removed.

- SmallMistake web site, at http://smallmistake.welcome.to, hosted pro-Israeli Attack Tool.
- Kala defaced the Netanya Academic College site, at http://mars.netanya.ac.il, in support of the Palestinians.

October 31, 2000:

- UNITY launched Phase 3 against ISP infrastructure in Israel, announced intentions to launch Phase 4 targeting "Zionist" e-Commerce sites, and distributed new tool among its members.
- m0r0n and nightman defaced the MBA International School of Business Administration Management site, at http://www.eiba.biu.ac.il, in support of the Palestinians.
- m0r0n and nightman defaced the MBA International School of Business Administration Management site, at http://www.mba.biu.ac.il, in support of the Palestinians.
- Israel radio claimed "an Internet site named Kill Israel, apparently operating from Saudi Arabia, is one of the main sources of the electronic onslaught on Israeli government sites."

November 1, 2000:

- Doctor Nuker broke into the American Israel Public Affairs Committee site, at http://www.aipac.org, and posted pro-Palestinian messages in addition to the credit card numbers and contact information of those who purchased items through the site, member contact information, and thousands of email addresses of individuals who signed up to receive email alerts.
- DeTH 'Sauron defaced Jarvis Entertainment Group's Web site, at http://www.gamingrevolution.com, with a message deriding both sides in the conflict: "Not many people realise the severity of the constant religious warfare and other CRAP that goes on in the middle east between Jews and arabs."

November 2, 2000:

- m0r0n and nightman defaced the site of Shenkar College, at http://www.shenkar.ac.il, in support of the Palestinians.

November 3, 2000:

- Cognifit Ltd. site, at http://www.cognifit.co.il, was defaced by dodi. The defacement urged pro-Palestinian attackers to target two DNS servers at NetVision with SYN flood attacks. dodi also said he was not only interested in Israeli targets but U.S. ones as well.
- Pakistan Hackerz Club (PHC) and GForce Pakistan joined the pro-Palestinian side.
- GForce Pakistan defaced Jen Communications site, at http://www.jen.co.il.

- GForce Pakistan defaced Health Infosystems Association, Israel site, at http://www.healthinfonet.co.il. Greetings were sent to rsh, hackweiser, m0r0n, nightman, doctornuker, phc, rootworm alldas, and attrition.
- GForce Pakistan defaced the Visiting Israel Students Association site, at http://www.visa.org.il.
- GForce Pakistan defaced the Pf1 Systems Ltd. site, at http://www.pf1.co.il.
- m0r0n and nightman defaced the site of the Yizrael Valley College (Mihlelet Emek Yizrael), at http://www.yvc.ac.il, in support of Palestine.
- GForce Pakistan defaced the site of the Jewish Bible Association, at http://www.jewishbible.org.
- GForce Pakistan defaced the Shema Yisrael Torah Network site, at http://shemayisrael.co.il.
- m0r0n and nightman defaced the Israeli Academic site http://www.yvc.ac.il.

November 4, 2000:

- m0r0n and nightman defaced Bayan Systems site, at http://www.bayan.co.il, in support of the Palestinians.
- m0r0n and nightman defaced Capit Ltd. site, at http://www.caspit.co.il, in support of the Palestinians.
- Lion&type_o ha k'eil defaced the site of the Iranian Ministry of Agriculture, at http://www.moa.or.ir, in support of the Israelis. Lion&type_o ha k'eil threatened to take down .ir and .lb sites and then .pk sites if GForce continued defacing .il sites.

November 5, 2000:

- GForce Pakistan defaced Jerusalem Books, at http://www.jerusalembooks.com, in support of the Palestinians.
- GForce Pakistan defaced Pirchei Shoshanim site, at http://www.pirchei.co.il, in support of the Palestinians.
- GForce Pakistan defaced the World Peace Center site, at http://www.worldpeacecenter.org, in support of the Palestinians.
- GForce Pakistan defaced the Ultimate Shabbat Site, at http://www.shabat.co.il, in support of the Palestinians.
- GForce Pakistan defaced Caspit Ltd. site, at http://www.caspit.co.il, in support of the Palestinians.
- GForce Pakistan defaced the All-Kosher Index, at http://www.kosher.co.il, in support of the Palestinians.
- GForce Pakistan, or a group claiming to be, defaced Shenkar College site, at http://www.shenkar.co.il, in support of the Palestinians.

November 6, 2000:

- Hackers of Israel Unite called for attacks against chats and ICQ, as well as the Palestinian National Authority, at http://www.pna.gov.ps, al-Manar, at http://www.almanar.com.lb, Palestine National Databank State Information Service, at http://www.sis.gov.ps, and Islamic Republic News Agency, at http://www.irna.com and www.albawaba.com.
- GForce Pakistan defaced the Borha Torah site, at http://www.borhatorah.org, in support of the Palestinians.
- GForce Pakistan defaced the Torah Educator site, at http://www.toraheducator.org, in support of the Palestinians.
- GForce Pakistan defaced the Partners in Torah site, at http://www.partnersintorah.org, in support of the Palestinians.

November 7, 2000:

- m0r0n and nightman defaced the Elgev Electronics site, at http://www.elgev.co.il, in support of the Palestinians.
- m0r0n and nightman defaced the Efrat DSP Group site, at http://www.efratdsp.co.il, in support of the Palestinians.
- HTTP Bomber 1.001b is believed to have been introduced into circulation.
- AnIcLaToR defaced the SofTech Tecnologia em Informatica LTDA site, at http://www.stn.com.br, advocating an end to the Israeli-Palestinian ground conflict.

November 8, 2000:

- "pakistan is gay" defaced URMIA site, at http://mail.urmia.ac.ir, in apparent retaliation for GForce Pakistan attacks against pro-Israeli sites.
- tR|cky, Boss, and KUCAU defaced Order in a Click site, at http://www.order-click.co.il, and Dilim Site, at www.dilim.co.il, in support of the Palestinians.
- m0r0n and nightman defaced the Hed-Arzi site, at http://www.hed-arzi.co.il, in support of the Palestinians.
- GForce Pakistan defaced the Ornetix site, at http://ntserver.ornetix.co.il, in support of the Palestinians. The defacement announced the addition of a new member to the group: nicks xtremist.
- GForce Pakistan defaced the Radwiz site, at http://www.radwiz.co.il. The defacement announced the addition of a new member to the group: nicks xtremist.
- Possible GForce Pakistan imposter defaced the KIS Technologies site, at http://www.kisnet.co.il. This defacement style did not fit GForce Pakistan's traditional form.
- Possible GForce Pakistan imposter defaced the Tel Aviv Chamber of Commerce site, at http://www.chamber.org.il, in support of the Palestinians. Once again, the defacement style did not fit GForce Pakistan's traditional form.

- GForce Pakistan defaced the Terminal-Computers & Multimedia site, at http://www.terminal.co.il. The group threatened attacks against DNS servers and NetVision in the defacement.
- GForce Pakistan defaced the Rooster site, at http://mail.rooster.co.il. The defacement threatened attacks against DNS servers and NetVision.
- m0r0n and nightman defaced the Gvanim Financim, Kibutz Shefayim Israel site, at http://www.gavnim.co.il, in support of the Palestinians.

November 9, 2000:

- AnIcLaToR defaced the U.S. Geological Survey site, at http://mrdata.usgs.gov, advocating an end to the Israeli-Palestinian ground conflict.

November 10, 2000:

- ReALiSt+ProjectGamma defaced the www.infinity.com.eg site in support of the Palestinians.
- tR|cky defaced the Western-Galilee College site, at http://wgalil.ac.il, in support of the Palestinians.
- Kuds launched coordinated HTTP Bomber 1.001b attacks against Israel.com site, at www.israel.com, beginning at 08:30 GMT.

November 11, 2000:

- m0r0n and nightman defaced the PC Center site, at http://www.pc-center.co.il.
- tR|cky and Boss defaced the Zefat Regional College site, at http://www.zrc.ac.co.il, in support of the Palestinians.
- tR|cky and Boss defaced the Open University-Jerusalem site, at http://www.jccopenu.ac.il, in support of the Palestinians.

November 12, 2000:

- m0r0n and nightman defaced the Lantronics Computer Networking Ltd. site, at http://www.lantronics.co.il, in support of the Palestinians.
- m0r0n and nightman defaced the Sivan-North Computer site, at http://www.sivan-north.co.il, in support of the Palestinians.
- lion&type_o defaced the www.primebank.com.pk site in support of the Israelis.
- lion&type_o defaced the Hafeez Center Global Internet Café site, at http://www.hafeezcentre.com.pk, in support of the Israelis.
- tR|cky and Boss defaced the Shavatz High School site, at http://www.savatz.givataim.k12.il, in support of the Palestinians.

November 13, 2000:

- m0r0n and nightman defaced the Tahal Group site, at http://www.tahal.co.il, in support of the Palestinians.

- m0r0n and nightman defaced the www.syscom.co.il site in support of the Palestinians.
- xZeroKiller defaced the Terminal-Computers & Multimedia site, at http://www.terminal.co.il, in a suspected pro-Palestinian attack.

November 14, 2000:

- m0r0n and nightman defaced the www.robotec.co.il site in support of the Palestinians.
- UnsecurityBR defaced the Terminal-Computers & Multimedia site, at http://www.terminal.co.il.

November 15, 2000:

- m0r0n and nightman defaced the www.topnet.co.il site in support of the Palestinians.
- m0r0n and nightman defaced topcom.topnet.co.il in support of the Palestinians.
- m0r0n and nightman defaced mail.topnet.co.il in support of the Palestinians.
- Murtaza Baloch, a.k.a. EdGe, defaced the www.karate.org.il site in support of the Palestinians.

November 18, 2000:

- Kuds, a pro-Palestinian group, launched coordinated HTTP Bomber 1.001b attacks against http://lgw.rotter.net.
- NETFORCE/PeRvErS defaced the Iranian Ministry of Foreign Affairs site, at http://www.mfa.gov.ir. It is not clear whether or not the defacement was in any way related to the Palestinian-Israeli conflict.
- tR|cky and petite_lourve defaced the Open University-Jerusalem site, at http://online.achva.ac.il, in support of the Palestinians.

November 19, 2000:

- The Iranian Ministry of Foreign Affairs site, at http://www.mfa.gov.ir, was defaced. It is not clear if the defacement was in any way related to the Palestinian-Israeli conflict. The defacer(s) posted the following message, "(HACKEADO POR USDL+{PH}+ BRASIL, greetz: L4ctus, SFx-1 e todos +{PH}+ ,securenet, hackernewsBRASIL... EU SOU BRASILEIRO COM MUITO ORGULHO APESAR DE TODA CORRUP€AO Q ENVOLVE ESTE PAIS. PLANET HACKER CLA ESTA COMIGO.)"
- tR|cky and xoid defaced the Open University-Jerusalem site, at http://www.jccopenu.ac.il, in support of the Palestinians.

November 25, 2000:

- Pro-Palestinian attackers launched a 3-hour coordinated assault against the Israel Ministry of Finance site, at http://www.mof.gov.il, and the email address webmaster@mof.gov.il.

November 26, 2000:

- m0sad defaced the Khaleej.com site, at http://www.khaleej.com, in support of the Israelis.

November 28, 2000:

- m0sad defaced Islam Web, at http://www.islamweb.net, in support of the Israelis.

November 29, 2000:

- m0sad defaced webhosting.ajeeb.com in support of the Israelis.

November 30, 2000:

- m0sad defaced the Sakhr Software Co. site, at http://www.ajeeb.com, in support of the Israelis.

December 1, 2000:

- m0r0n and nightman defaced SOMA Galleries, at http://www.somagalleries.com, in support of the Palestinians. The defacement team also announced that the duo had joined the World's Fantabulous defacers (WFD).
- Israel Land Administration site was forced to close down most of its site due to cyber attacks. Attacks began in the middle of the week but eventually overwhelmed the site on the December 1, 2000.

December 2, 2000:

- [^CyBeRpUnK^] defaced the Hebrew University of Jerusalem, Israel site, at http://shemesh.fiz.huji.ac.il, with a pro-peace message.
- [^CyBeRpUnK^] defaced the www.as.huji.ac.il site with a pro-peace message.
- m0sad defaced www.talkislam.com in support of the Israelis.

December 3, 2000:

- m0r0n and nightman defaced www.comune.scandiano.re.it in support of the Palestinians.
- m0sad defaced the Ministry of Awqaf and Islamic Affairs, Qatar site, at http://www.islam.gov.qa, in support of the Israelis.

December 5, 2000:

- m0r0n and nightman, of WFD, defaced the Haifa University Campus Network site, at http://modiin.haifa.ac.il, in support of the Palestinians.
- B_Real and BrakeOFF defaced the Los Alamos Neutron Science Center site, at http://www.lansce.lanl.gov, in support of the Palestinians.

December 7, 2000:

- m0r0n and nightman, of WFD, defaced the Volasia Ltd. site, at http://www.volasia.com, in support of the Palestinians.
- [^CyBeRpUnK^], of WFD, defaced admin-scb.ouhsc.edu in support of the Palestinians. [^CyBeRpUnK^] made an offer of cooperation to Doctor Nuker in this defacement.

December 8, 2000:

- B_Real and BrakeOFF defaced www.cruzazul.com.mx in support of the Palestinians.

December 9, 2000:

- SomeOneFromHeaven (SoFh), of WFD, defaced www.cowboysorlando.com in support of the Palestinians.
- SomeOneFromHeaven (SoFh), of WFD, defaced the Christian Sharing Center site, at http://www.christiansharing.org, in support of the Palestinians.
- SomeOneFromHeaven (SoFh), of WFD, defaced the Central Florida Bankruptcy Law Association site, at http://www.cfbla.org, in support of the Palestinians.
- [^CyBeRpUnK^] and nightman, of WFD, defaced albert.ph.biu.ac.il in support of the Palestinians.
- m0r0n and nightman, of WFD, defaced the University Medical Center Nijmegen Dept. of Urology, Netherlands site, at http://uroworld.azn.nl, in support of the Palestinians.

December 10, 2000:

- m0r0n and nightman, of WFD, defaced www.pccua.cc.ar.us in support of the Palestinians.
- m0sad defaced the United Arab Emirates Dept. of Civil Aviation site, at http://www.dcaauh.gov.ae, in support of the Israelis.
- BrakeOFF defaced www.corpac.gob.pe in support of the Palestinians.
- BrakeOFF defaced sgl1.lanres.com in support of the Palestinians.
- BrakeOFF defaced the ARON site, at http://www.aron.be, in support of the Palestinians.

December 11, 2000:

- h3ll rais3r and laughing3y3s, of WFD, defaced www.asbis.sk in support of the Palestinians.
- SomeOneFromHeaven (SoFh), of WFD, defaced www.al-libaas.com in support of the Palestinians.

December 12, 2000:

- m0r0n and nightman, of WFD, defaced the Wisconsin K12 Schools site, at http://www.sharon.k12.wi.us, in support of the Palestinians.

- [^CyBeRpUnK^] and nightman, of WFD, defaced the Hebrew University of Jerusalem, Israel site, at http://www.music.md.huji.ac.il, in support of the Palestinians.
- m0sad defaced the Iranian Foreign Ministry site, at http://mfa.gov.ir, in support of the Israelis.

December 13, 2000:

- SomeOneFromHeaven (SoFh), of WFD, defaced Lymphedema Awareness Foundation site, at http://www.lymphaware.org, in support of the Palestinians.
- WFD defaced the Hebrew University of Jerusalem, Israel site, at http://daat.ls.huji.ac.il, in support of the Palestinians.

December 14, 2000:

- BrakeOFF defaced www3.co.oakland.mi.us in support of the Palestinians.

December 15, 2000:

- m0sad defaced the Talk Islam, Library of Islamic Web Sites, at http://www.talkislam.com, in support of the Israelis.

December 16, 2000:

- m0r0n and nightman, of WFD, defaced www.ann-arbor.med.va.gov in support of the Palestinians.
- m0r0n and nightman, of WFD, defaced www.dol.wa.gov in support of the Palestinians.
- h3ll rais3r and laughing3y3s, of WFD, defaced the AMTEL Slovensko Ltd. site, at http://www.amtel.sk, in support of the Palestinians.
- Tå|{ê Ñø £Øgîç, of WFD, defaced the Malaysian Rubber Board site, at http://www.lgm.gov.my, in support of the Palestinians.

December 17, 2000:

- EdGe defaced the Server Computers site, at http://www.netserver.co.il, in support of the Palestinians.
- m0r0n and nightman, of WFD, defaced the Karnataka Telecom Circle site, at http://www.karnataka.dotindia.com, in support of the Palestinians.
- GForce Pakistan defaced the Indian Institute of Science Materials Research Center site, at http://arun.mrc.iisc.ernet.in, in support of the Palestinians.
- GForce Pakistan defaced the Indian Institute of Science Dept. of Mechanical Engineering site, at http://mecheng.iisc.ernet.in, in support of the Palestinians.

December 18, 2000:

- m0r0n and nightman, of WFD, defaced the BSNL Nagpur (Dept. of Telecom) site, at http://nagpur.dotindia.com, in support of the Palestinians.

- Tå|{ê Ñø £Øgîç, of WFD, defaced the Kuala Lumpur Department of Urban Transportation site, at http://www.jpbdbkl.gov.my, in support of the Palestinians.
- GForce Pakistan defaced the Dizasta Productions site, at http://www.dizasta.net, in support of the Palestinians.

December 19, 2000:

- m0sad defaced the Islamic University, Gaza site, at http://www.iugaza.edu, in support of the Israelis.
- m0sad defaced the Islamic Society of North America site, at http://www.isna.net, in support of the Israelis.
- BrakeOff defaced the Qatar Ministry of Awqaf and Islamic Affairs, at http://www.islam.gov.qa, in support of the Palestinians.
- Laughing3y3s and h3ll rais3r, of WFD, defaced shop.chemolak.sk in support of the Palestinians.
- Laughing3y3s and h3ll rais3r, of WFD, defaced www.cardcentrum.sk in support of the Palestinians.
- SomeOneFromHeaven (SoFh), of WFD, defaced United Studios Corp., at http://www.usidentity.com, in support of the Palestinians.
- m0r0n and nightman, of WFD, defaced the Kolhapur Telecom District site, at http://www.kolhapur.dotindia.com, in support of the Palestinians.
- Tå|{ê Ñø £Øgîç, of WFD, defaced the Scicom site, at http://www.scicom.com.my, in support of the Palestinians.
- GForce Pakistan defaced Web of India site, at http://webmail.webindia.com, in support of the Palestinians.
- GForce Pakistan defaced Web of India site, at http://tanishq.webindia.com, in support of the Palestinians.
- GForce Pakistan defaced Web of India site, at http://servlet.webindia.com, in support of the Palestinians.
- GForce Pakistan defaced Web of India site, at http://servlet2.keralatourism.org, in support of the Palestinians.
- GForce Pakistan defaced Web of India site, at http://dmss.webindia.com, in support of the Palestinians.
- [^CyBeRpUnK^], of WFD, defaced the KAIZ site, at http://www.kaiz.com, in support of the Palestinians.

December 20, 2000:

- m0r0n and nightman defaced the Ardom Telecomputing of Israel site, at http://www.ardom.co.il, in support of the Palestinians.
- GForce Pakistan defaced www.xmlprobe.com in support of the Palestinians.
- GForce Pakistan defaced the University of Chicago Computer Science Dept. site, at http://hamachi.cs.uchicago.edu/, in support of the Palestinians.

- Kr4kr0k Industries defaced Arttalk.com, at http://www.arttalk.com, in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.hmcnet.com in support of the Palestinians.

December 21, 2000:

- m0r0n and nightman, of WFD, defaced www.aztek.co.il in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.stadtklima.de in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.cog.co.jp in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced the University of North Texas site, at http://www2.music.unt.edu, in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.desisti.it in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.929rtl.at in support of the Palestinians.

December 22, 2000:

- EDGE & KARTOOS.AK.47 defaced www.tamtravel.com in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.pryor.k12.ok.us in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.carroll.k12.ga.us in support of the Palestinians.
- GForce Pakistan defaced the Merical (IN) site, at http://email.merical.ac.in, in support of the Palestinians.
- ConClaveCrew defaced the Sheffield Hallam University site, at http://jeff.sci.shu.ac.uk, with a pro-peace message.

December 23, 2000:

- m0r0n and nightman, of WFD, defaced the Centers for Disease Control and Prevention (CDC) site, at http://phil.cdc.gov, in support of the Palestinians.
- h3ll rais3r and laughing3y3s, of WFD, defaced the Forma Ltd. site, at http://www.deiure.sk, in support of the Palestinians.
- GForce Pakistan defaced #2 National Centre for Radio Astrophysics site, at http://sakthi.ncra.tifr.res.in, in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced the Frostbit.com site, at http://www.frostbit.com, in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.nbas.cz in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.cursobolsa in support of the Palestinians.

- EDGE & KARTOOS.AK.47 defaced the Deutsche Forschungsanstalt fuer Luft – und Raumfahrt e.V. (DLR) site, at http://www.weblab.dlr.de, in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.s-scptuj.mb.edus.si in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced the #3 Lal Bahadur Shastri National Academy of Administration, Mussoorie, at http://www.lbsnaa.ernet.in, in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced dns0.whuci.edu.cn in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.whuci.edu.cn in support of the Palestinians.

December 24, 2000:

- H3ll rais3r and laughing3y3s, of WFD, defaced the Compact Studio site, at http://www.dvdbest.sk, in support of the Palestinians.
- GForce Pakistan defaced the Indian Institute of Science Dept. of Metallurgy, at http://www.metalrg.iisc.ernet.in, in support of the Palestinians.
- GForce Pakistan defaced delhinms.mtnl.net.in in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.scjh.kh.edu.tw in support of the Palestinians.
- EDGE & KARTOOS.AK.47 defaced www.retliv.com in support of the Palestinians.

December 25, 2000:

- WFD defaced the Pelenews site, at http://www.pelenews.co.il, in support of the Palestinians.
- Kashmir Hackers Club (KHC) defaced www.microconnectors.com in support of the Palestinians.
- GForce Pakistan defaced the Indian Institute of Science Solid State and Structural Chemistry Unit site, at http://zeolite.sscu.iisc.ernet.in, in support of the Palestinians.

December 26, 2000:

- Hezbollah site, at http://www.hizbollah.org, was defaced by pro-Israeli attacker.
- m0r0n and nightman, of WFD, defaced the Anti-Defamation League (ADL) site, at http://www.adl.org, in support of the Palestinians.
- m0r0n, nightman, and fighter4Isl@m, of WFD, defaced www.dilim.co.il in support of the Palestinians. This defacement marked the announcement signaling the beginning of Phase 5 of the cyberconflict.

December 27, 2000:

- m0r0n, nightman, and fighter4Isl@m, of WFD, defaced www.order-click.co.il in support of the Palestinians. This defacement marked the announcement signaling the beginning of Phase 5 of the cyberconflict.
- GForce Pakistan defaced the Rabia Gupta Design site, at http://www.styletantra.com, in support of the Palestinians.

December 28, 2000:

- EDGE & KARTOOS.AK.47 defaced the sira1.sira.it in support of the Palestinians. The defacement announced the formation of THE SCYTHE by the two attackers.

December 29, 2000:

- A massive Internet attack almost entirely destroyed 80 Israeli Web sites.

Both pro-Palestinian and pro-Israeli actors have continued to utilize computer network systems and the Internet as a weapon against one another. Although the extent to which actors have utilized defacements, denial-of-service attacks, viruses, and other CNO has drastically decreased since the Palestinian-Israeli Cyberconflict of 2000, the following list provides examples of CNO incidents which have taken place since the beginning of 2001:

March 20, 2001:

- Palestinians sent the first politically motivated mass mailing computer virus, “Injustice.”

March 29, 2002 – April 22, 2002:

- Israel was the victim of 10 significant computer hacking incidents. During this time, only 15 such attacks were recorded throughout all of the Middle East.

June 2002:

- Pro-Islamic group Unix Security Guards made 20 attacks on corporate and government computer systems worldwide as part of their increased activity to highlight the Palestinian cause.

July 2002:

- Pro-Islamic group USG made 27 attacks on corporate and government computer systems worldwide as part of their increased activity to highlight the Palestinian cause.

August 2002:

- Pro-Islamic hacker group USG made 21 attacks on corporate and government computer systems worldwide as part of their increased activity to highlight the Palestinian cause.

September 2002:

- Pro-Islamic hacker group USG made 207 attacks on corporate and government computer systems worldwide as part of their increased activity to highlight the Palestinian cause.

November 2002:

- The Web sites and e-mail of pro-Palestinian advocacy groups and prominent supporters, to include Noam Chomsky and Francis Boyle, within the U.S. were disrupted and/or eliminated by suspected pro-Israel groups.

October 6, 2003:

- It was reported on October 6, 2003, that over 500 digital attacks took place over the weekend on British, American, and Norwegian Internet sites to protest against the Israeli attacks on an alleged terrorist camp in Syria as well as residential compounds in Palestine.

H. OBSERVATIONS AND CONCLUSIONS OF THE PALESTINIAN-ISRAELI CYBERCONFLICT

Many have claimed that the Palestinian-Israeli Cyberconflict of 2000 is the first example of a political conflict waged over the Internet in an organized fashion by two opposing sides. Evidence indicates that both specialized hackers and average citizens, throughout the world, participated in what became a series of defacements, denial-of-service attacks, e-commerce disruptions, and cyberterror threats. The extent to which each side was able to disrupt, degrade, exploit, deny, and/or destroy the adversary's capabilities will most likely never be fully understood; however, it is safe to assume that the events which occurred during a four-month span at the end of 2000 caused millions of dollars in "clean-up," security, and manpower, not to mention hours of annoyance, and provided a glimpse of things to come in the realm of cyberwarfare. As one commentator speculated about the future impact of the Palestinian-Israeli Cyberconflict, "In the broader scheme of things, the Arab-Israeli cyber war offers a window into the kind of threats that leading economic powers will face in the twenty-first century. IT experts at the Pentagon have reportedly been preparing for precisely these kinds of attacks for years and are watching the situation closely."[82]

Pro-Palestinian actors utilized computer network systems and the Internet during the al-Aqsa Intifada in a similar fashion to their use of the media during the First Intifada. In addition to television and the print media, computers and the Internet provided the pro-Palestinian movement with an outlet for political expression, a media through which to mobilize Palestinian and international support, an arena in which to erode support for Israel, and what proved to be both a viable weapon and opportunistic target of attack. The use of personal computers, laptops, and Internet cafés allowed pro-Palestinian actors to overwhelm Israel, what many consider to be a well trained and equipped, militarily superior force, economically and technologically advanced society, led by an established and organized governing body. In fact, Israel's superior connectivity and computer literacy may have made it an easier target of attack, with its government, military, academia, infrastructure, and economy reliant upon computer network systems and the Internet for operations and connectivity. The scope of the conflict extended beyond the borders established by the physical conflict, including attacks to and from Israel, Palestine, Lebanon, Jordan, Pakistan, Egypt, the U.S., and others. Participants included skilled hackers as well as average computer users, in particular a young population using personal computers in their homes or from Internet cafes.

The difficulty to clearly define actors in cyberspace and a lack of legal framework from which to seek retribution created a nebulous threat of direct retaliation by Israel against pro-Palestinian actors. The wide distribution of participants, with little if any "hierarchical coordination," favored the pro-Palestinian effort by diminishing the risk of direct retaliation by the Israelis.[83] Likewise, the difficulty of defining actors clearly and accurately in cyberspace prohibited Israel from taking targeted action against pro-Palestinian aggressors. As a result, if anything, the Palestinian-Israeli Cyberconflict,

[82] Gary C. Gambill, "Who's Winning the Arab-Israeli Cyber War?" *Middle East Intelligence Bulletin* (November 2000), http://www.meib.org.

[83] Sean Lawson, "The Cyber-Intifada: Activism, Hactivism, and Cyber-Terrorism in the Context of the "New Terrorism."" Prepared as a seminar paper for the course, Information Warfare and Security, taught by Dorothy Denning, Georgetown University, Fall 2001, pp. 9-11.

while lacking in mass physical destruction and casualties, proves that computer network systems and the Internet are becoming viable tools of warfare.

While many computer experts and security analysts consider the Palestinian-Israeli Cyberconflict a victory, in terms of successful attacks, for the pro-Palestinian movement, little "on the ground" progress was gained from this series of cyberspace battles. Israel remains a militarily, financially, and technologically superior society. It hosts a recognized and elected, organized governing body which is able to conduct operations domestically and internationally. Even with the success of their Internet campaign, local Palestinian access to the Internet was very limited and what access was available relied for the most part on English and/or other Western languages, not Arabic. The limited protocols and Internet infrastructure explain why some pro-Palestinian and pro-Israeli actors claimed responsibility for their defacements and attacks in English, not Hebrew or Arabic. In addition to the "linguistic infrastructure barriers," the primary mode of connecting to the Internet in the Palestinian Territories was via phone lines and modems dependent on Israel's infrastructure.[84] As a result, phone access and therefore Internet access could be controlled, manipulated, and interrupted by Israelis. Combine these infrastructure barriers with the limited diffusion of the Internet in the Palestinian Territories, and it becomes obvious that the vast majority of Palestinians within the Palestinian Territories were unable to participate in the Palestinian-Israeli Cyberconflict. Despite these limitations, participation by financially able NGOs and the Palestinian Authority were able to overcome these infrastructure barriers. Only time will tell what future benefits may come from increasing Internet infrastructure throughout the Palestinian population.

The pro-Palestinian movement proved its ability to attack a superior state's government, military, economy, and/or infrastructure via CNO. By disrupting Israeli society via CNO, the pro-Palestinian actors proved their ability as a potential, if not superior, foe within the cyberspace battlefield. While no significant attacks to the economy, military, government, and/or infrastructure occurred, the pro-Palestinian

[84] W. Sean McLaughlin, "E-Intifada: Internet in the Palestinian Uprising," Foundations, 2001-2002, p. 39.

movement successfully caused an estimated 8% drop in the Tel Aviv Stock Exchange, contributed to Israeli uncertainty regarding the reliability and security of Internet access and computer network systems in the state, led many businesses (to include the IDF) to seek assistance from international security corporations and ISPs, and may have compromised sensitive information. Had any single entity attempted a more serious attack, the consequences may have been catastrophic. The very nature of this conflict illustrates the potential of CNO to level the battlefield in future asymmetric conflicts, for as Tim Bass, President and CEO of security consulting firm The Silk Road Group, wrote, "Adversaries in asymmetrical conflicts are at an advantage in cyberspace because no one dominates, and those in power and authority have only primitive situational knowledge."[85]

[85] Daniel Verton, "New Cyberterror Threatens AF," Federal Computer Week, May 3, 1999, www.fcw.com, last accessed August 12, 2005.

V. EFFECTS AND RAMIFICATIONS OF COMPUTER NETWORK OPERATIONS ON THE U.S.

According to the "Third Wave" theory purported by the Tofflers, information ascends to become the most important resource and, as such, becomes a significant means of preventing and/or limiting future wars, as well as wining them. While many scoff at such a notion, we cannot deny that victorious forces throughout the ages have relied on information superiority to attain the battlefield advantage. Conflicts may not necessarily be waged only in cyberspace, but it is important to recognize that

> the American military is the most information-dependent force in the world. It uses computers to help design weapons, guide missiles, pay soldiers, manage medical supplies, write memos, control radio networks, train tank crews, mobilize reservists, issue press releases, find spare parts, and even suggest tactics to combat commanders.[86]

The American military is claimed to be the most networked force in the world, a combination which, absent adequate defenses, makes the American military, and thus the American populace, extremely vulnerable to information attacks.[87] Add to that the United States' dependence on computers and computer networks for banking, communication, stock exchanges, transportation, and air traffic control; it becomes obvious that, in the words of Vice Admiral John McConnell, former Director of the National Security Agency, "we've become the most vulnerable nation on earth."[88] In 1995, the Joint Security Commission characterized the American vulnerability to infowar as "the major security challenge of this decade and possibly the next century."[89] In light of such a security vulnerability, individuals, terrorists, and/or foreign countries capable of

[86] *Washington Post,* "The Pentagon's New Nightmare: An Electronic Pearl Harbor," July 16, 1996, p. C03.

[87] Richard W. Aldrich, *The International Legal Implications of Information Warfare*, U.S. Air Force Institute for National Security Studies Occasional Paper 9, http://www.usafa.af.mil/df/inss/OCP/ocp9.pdf, (April, 1996), vi and 2.

[88] *Time*, "Onward Cyber Soldiers," August 21, 1995, p. 44.

[89] *Time*, "Onward Cyber Soldiers," August 21, 1995, p. 40.

penetrating U.S. networks and information systems could wreak havoc throughout U.S. defense systems, communications capabilities, power grids, emergency response units, and banking, just to mention a few.

A. CNO INCIDENTS IN/AGAINST THE U.S.

As the most computer literate and technologically savvy society, the U.S. is home to many individuals capable of waging CNO and a number of targets vulnerable to CNO. Since the advent of personal computers and the Internet, the U.S. has found itself in a race to remain technologically superior to our allies and adversaries. Unfortunately, as the Palestinian-Israeli Cyberconflict indicates, technologically superior states, which have become reliant upon computer network systems and the Internet, make themselves vulnerable targets for CNO exploits. As stated by former Defense Secretary William Cohen, "If you can shut down our financial system, if you could shut down our transportation system, if you could cause the collapse of our energy production and distribution system just by typing on a computer and causing those links to this globalization to break down, then you're able to wage successful warfare, and we have to be able to defend against that."[90] The following examples illustrate CNO, and relevant events, which have taken place in and against the U.S.:

- In March 1994, system administrators at Rome Lab in New York found their network under an attack which was traced to an ISP first in New York, then in Seattle, Washington, where the Internet path dead-ended. Datastream Cowboy, a 16 year-old British student, later pled guilty and was fined. His mentor, Kuji, a 22 year-old Israeli information technology specialist was found not guilty because no laws in Israel applied to this incident.[91]
- In 1997, 35 people participated on the Red Team over 90 days using off-the-shelf technology and software as part of Eligible Receiver, the first IW exercise in the U.S. The scenario was a rogue state rejecting direct military confrontation with the U.S., while seeking to attack vulnerable U.S. information systems. A number of simulated cyber attacks were carried out against power and

[90] Dan Verton, "Superpower Status Risks Cyber attack," Feceral Computer Week, August 24, 2000, www.fcw.com, last accessed August 12, 2005.

[91] Steven A. Hildreth, "Cyberwarfare," CRS Report for Congress, June 12, 2001, p. 4.

communications networks in Oahu, Los Angeles, Colorado Springs, St. Louis, Chicago, Detroit, Washington, D.C., Fayetteville, and Tampa. Gen. Campbell, former head of the Pentagon's joint Task Force – Computer Network Defense, wrote that Eligible Receiver "clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure."[92]

- In February 1998, a number of Department of Defense networks were attacked using a well-known vulnerability in the Solaris (UNIX-based) computer system. The attackers probed Defense Department servers to see if the vulnerability existed, exploited the vulnerability and entered the system, planted a program to gather data, and then returned later to collect that data. While initial activities appeared to originate from Harvard University and the United Arab Emirates, moving on to Pearl Harbor and a number of Air Force bases; in the end, two California high school students were arrested and pled guilty, and their mentor, an 18 year-old Israeli, was arrested and indicted. In all, over 500 computer systems were compromised, including military, commercial, and educational sites, by attackers using only moderately sophisticated tools.[93]
- In 1998, Ehud Tennenbaum, a.k.a. "the Analyzer," an Israeli hacker, penetrated classified computer systems at an estimated 400 U.S. military sites, including the Pentagon.
- On October 31, 2000, UNITY launched Phase 3, its denial-of-service campaign. Through obscure hacker chat rooms and encrypted e-mail messages, pro-Palestinian actors from around the world were directed to a UNITY website, from which they were automatically redirected to another site and greeted with a call to action. Of their suggested targets, No. 12, the New Jersey based Lucent Technologies sent warning flags to businesses across the Atlantic.
- In November 2000, UNITY claimed in an e-mail to have successfully attacked AT&T in retaliation for the services it provided to the IDF. In the e-

[92] Steven A. Hildreth, "Cyberwarfare," CRS Report for Congress, June 12, 2001, p. 4.

[93] Ibid.

mail, a UNITY representative stated, "We have used the DoS attack against them and we were successful three times, [with] one of them the site was blocked about 72 hours." When questioned, AT&T declined to comment.[94]

- In November 2000, reports surfaced alleging that the Pentagon had considered using cyberattacks to infiltrate and/or liquidate Serbia's financial systems during the Kosovo Conflict. In January 2001, *Newsweek* reported that President Clinton had issued a highly classified "finding" authorizing the CIA to use its particular talents to school Kosovar rebels in the art of sabotage. The article further alleged that the president ordered the CIA to use its hacking skills to penetrate the international banking system and loot Serbian President Slobodan Milosevic's bank accounts in Russia, Cyprus, and Greece.[95] It is said to have backed off, partly because of the ambiguity of international law, and partly because of fears that such weapons, if used, could easily be adopted by America's enemies.

- On November 1, 2000, Doctor Nuker, founder of the Pakistan Hackerz Club, attacked the American Israel Public Affairs Committee (AIPAC), a pro-Israel lobbying group. Doctor Nuker not only defaced the site, but also downloaded the credit card details of approximately 700 people (including a Republican senator) who had subscribed to AIPAC via the Internet.

- After Doctor Nuker's penetration of the American Israel Public Affairs Committee on November 1, 2000, the FBI's National Infrastructure Protection Center (NIPC) warned that such digital activism had been and would continue to be a fallout of the violent clashes between Israelis and Palestinians. According to an advisory at the NIPC site, "The recent unrest in the Middle East appears to have been responsible for an increase in cyber attack activity between sympathizers on both sides of the tensions. Known targets have included

[94] John Galvin, "The Real Online Battleground: There's Another World War Brewing, and Most of Us Don't Even Know It," ZdNet News, February 7, 2001, http://www.zdnet.com/, last accessed February 7, 2001.

[95] Kevin Poulson, ZDNet News, January 22, 2001, http://news.zdnet.com2100-9595_22-514749.html, last accessed August 12, 2005.

websites operated by the Israeli government and military as well as websites operated by pro-Palestinian organizations including Hizballah and Hamas."[96]

- Another advisory from the FBI's cybercrime unit stated, "Due to the credible threat of terrorist acts in the Middle East region, and the conduct of these Web attacks, (Internet users) should exercise increased vigilance to the possibility that U.S. government and private-sector Web sites may become potential targets." The FBI recommended security measures for government agencies and private businesses to prevent e-mail flood attacks, block source e-mail addresses in the event of a flooding, and ensure that appropriate patches were installed in operating systems to limit vulnerability to other denial-of-service attack methods.[97]
- On November 2, 2000, Lucent Technologies, based in Murray Hill, New Jersey, confirmed that its website was the victim of at least one attack by pro-Palestinian hackers.[98]
- In an article published on November 10, 2000, security-information company LogiKeep Inc. said that notes posted in anti-Israel site defacements indicated that attacks against the AT&T telecommunications company were planned. A message on the AT&T site, from the group GForce Pakistan, suggested that the group was planning to reroute traffic from AT&T to competitor Qwest Communications International Inc.[99]
- The U.S.-China cyber skirmish of May 2001 shared similar features with the Palestinian-Israeli Cyberconflict. During the attack, hackers came very close to disrupting electricity transmissions in California; if successful, the cost to Californians and to the U.S. in national prestige and security would have been

[96] Jennifer Disabatino, "Pro-Israel Web Site Hacked by Pro-Palestinian Cracker," *Network World*, November 6, 2000, http://www.nexis.com, last accessed April 26, 2005.

[97] Ranwa Yehia, "Hackers Launch Phase Three of Online Intifada," *The Daily Star*, November 4, 2000, http://www.dailystar.com.lb/04_11_00/art4.htm, last accessed November 6, 2000.

[98] John Lancaster, "Abroad at Home: Mideast Hacker Wars Hit U.S. Group's Site," The Washington Post, November 3, 2000, p. A31, http://washingtonpost.com/wp-dyn/articles/A4288-2000Nov2.html, last accessed November 3, 2000.

[99] Barnaby Page, "Pro-Palestinian Hackers Threaten AT&T," TechWeb.com, November 10, 2000, http://www.techweb.com/wire/29116059, last accessed August 12, 2005.

immense. During this period, Chinese hackers successfully penetrated a test network of a California electric power transmission company.[100]

- Soon after the September 11, 2001 attacks on the U.S., GForce Pakistan defaced a server belonging to the U.S. National Oceanic and Atmospheric Agency and threatened to target U.S. and British military sites.[101]
- In 2002, The Washington Post reported that U.S. intelligence services had monitored al-Qaeda terrorists snooping around in the computer systems of dams, power plants, and other facilities.
- In July 2005, Gary McKinnon, a British citizen, was accused of accessing 97 U.S. government computers, causing an estimated $700,000 in damages. McKinnon deleted files that shut down more than 2,000 computers in the U.S. Army's military district of Washington, D.C. for 24 hours "significantly disrupting governmental function." Reports claim that McKinnon left a note on an army computer in 2002 saying U.S. foreign policy was "akin to government-sponsored terrorism" The note allegedly said, "It is not a mistake that there was a huge security stand down on September 11 last year. I am Solo. I will continue to disrupt at the highest levels." McKinnon is accused of 20 counts relating to the U.S. Army, Navy, and Air Force, NASA, and the Department of Defense.[102]
- On July 21, 2005, authorities discovered a breach of the San Diego County Employees Retirement Association. The targeted servers contained the names, Social Security numbers, addresses, and dates of birth of current and former county employees. The breach may have provided hackers with access to personal data belonging to approximately 33,000 people enrolled in San Diego County's retirement plan.[103]

[100] Patrick D. Allen and Chris C. Demchak, "The Palestinian-Israeli Cyberwar," Military Review, March-April 2003, p. 52.

[101] "Israel Under Hack Attack," BBC News, April 16, 2002, http://www.infowar-monitor.net, last accessed August 28, 2005.

[102] Catriona Davies, "U.S. Army Computers 'Shut Down by Hacker'," news.telegraph, July 28, 2005, last accessed August 11, 2005.

[103] "Hackers Target County's Retirement Plan," 10news.com, July 31, 2005, last accessed August 24, 2005.

B. U.S. WEAKNESSES

While technologically superior, the U.S. has become vulnerable to CNO. Despite efforts by the government, military, and research and development sectors to bolster our defensive and offensive CNO capabilities, a number of weaknesses remain. Unfortunately, while our government, military, academia, business, and financial markets continue to rely on products developed by and distributed on the open market, individuals and groups will continue to find vulnerabilities in our systems. Additionally, a lack of codified national and international laws regarding cyberspace continues to limit the U.S.'s ability to pursue and prosecute computer criminals. Technical, legal, privacy and even political challenges curtail our ability to counter cybercrime and cyberterrorism, and government efforts remain hampered by civil liberties concerns. The following provide just a few examples to illustrate U.S. weaknesses which continue to make our military, commerce, and infrastructure – our national security – vulnerable to CNO:

- Many, if not most, targets of an attack against the U.S. will probably be commercial computer and communications systems, which are more vulnerable than those operated by the military. Although commercial information systems are prime targets for attack, the government has limited influence over how these systems are designed, manufactured, and operated. Key points of contention between government and industry include: antitrust, encryption, criminal investigations, civil liberties, and immigration laws. Unless government officials and industry improve relations, the U.S. will become increasingly vulnerable as it becomes more dependent on computers, the systems which operate them, and the networks that interconnect them.
- The U.S. government has been hampered in its efforts to monitor and track terror conversations and data transfers on the Internet by privacy concerns and civil liberties. For example, in 2003, the U.S. Senate pulled funding from the Pentagon's anti-terror data-mining project, which was intended to "mine data" by searching everything from credit cards and medical records, to travel information, e-mail, bank deposits, and even magazine descriptions, to uncover suspected terrorists. Civil libertarians also attacked an effort to track terrorists' use of U.S.

air travel, an updated version of Washington's Computer Assisted Passenger Prescreening System, which would create a new passenger-screening database that would be able to check every domestic U.S. traveler's credit history, arrest record, and property-tax data.[104] There is no universal rating system in effect, and none is mandated, that would make filtering-software products chosen by consumers more effective. Additionally, laws aimed at allowing tighter filtering, not to mention mandating it, such as the Communications Decency Act and the Children's Online Protection Act, have already been struck down in courts based on First Amendment grounds. Thus, Internet content remains largely unregulated and the public remains vulnerable to attack.

- Malicious computer code that attacks information systems may be treated as a weapon of war within the scope of the laws of armed conflict, and attempts have been made by international organizations to classify and control malicious code. Despite proposals by Russia, the Council of Europe's Cybercrime Convention, and the G-8 Government-Industry Conference on High Tech Crime to seek international agreement on ways to classify and control malicious computer code and/or the need for arms controls for information warfare weapons, the Department of Defense has yet to develop a policy regarding international controls for cyberweapons. The debate on whether to pursue international agreements to codify cybercrime legislation and to deter cybercrime through more stringent criminal penalties remains prominent. The combination of technical problems of pursuit and/or detection "are made increasingly complex if one or more of the nations involved has a legal policy or political ideology that conflicts with that of the United States."[105]

[104] Alan D. Abbey, "Virtual Jihad," The Jerusalem Post, May 8, 2004, http://www.infowar-monitor.net, last accessed August 28, 2005.

[105] Clay Wilson, "Information Warfare and Cyberwar: Capabilities and Related Policy Issues," CRS Report for Congress, July 19, 2004, pp. 11-12.

VI. CONCLUSION AND RECOMMENDATIONS

Recent U.S. administrations have made progress in defining the use of CNO and securing computer network systems and the Internet for users, commerce, academia, the military and government. The Bush Administration has taken a number of encouraging steps towards securing the U.S. against cyberthreats, while utilizing this technology to its fullest extent. In 2002, President Bush signed the National Security Presidential Directive 16, which was intended to clarify circumstances under which a CNO attack would be justified and who has the authority to launch a computer attack.[106] In 2004, President Bush encouraged U.S. adoption of the Council of Europe Cybercrime Treaty, which would require participating nations to update their laws to reflect computer crimes such as unauthorized intrusions into networks, the release of worms and viruses, and copyright infringement. The Treaty also includes arrangements for mutual assistance and extradition among participating nations.[107] Additionally, President Bush proposed funding the Department of Homeland Security's National Cyber Security Division with an $80 million budget. The Bush Administration recognizes the importance of computer network systems and the Internet, and the necessity to protect this vital interest, "Cyberspace security is a key element of infrastructure protection, because the Internet and other computer systems link many infrastructure sectors…The consequences of a cyber attack could cascade across the economy, imperiling public safety and national security."[108]

President Bush's call to develop a "National Strategy to Secure Cyberspace" has become very relevant in today's society. Much of our infrastructure, economy, research, and livelihood currently rely (at least in some part) on the network of users, computers, and systems, known as the Internet. The development of the Internet allowed academia to share research and ideas in a real-time open forum, in which coordination and debate

[106] Clay Wilson, "Information Warfare and Cyberwar: Capabilities and Related Policy Issues," CRS Report for Congress, July 19, 2004, p.10.

[107] Clay Wilson, "Information Warfare and Cyberwar: Capabilities and Related Policy Issues," CRS Report for Congress, July 19, 2004, p.12.

[108] White House analysis released with the fiscal 2005 U.S. Budget Proposal.

contributed to the sciences, technology, and the dissemination of information. Unfortunately, as with all good things, society has found ways to manipulate and corrupt the Internet. Internet users currently find their email inboxes flooded with "spam," their browser windows cluttered with "pop-ups," their computer systems infiltrated by "backdoors," their hard-drives infected by "worms," "Trojan horses," and "viruses." It is only a matter of time before terrorists utilize the Internet to attack critical infrastructure. Unlike territorial borders and sovereign nations, the information superhighway is a global network of computers, users, and corruption. Lacking boundaries, legal ramifications, and the ability to seek retribution; the Internet has become an easy weapon in today's modern wars.

In an attempt to prevent, secure, and defend America's infrastructure, economy, and livelihood – our national security; President Bush appointed members to the President's Critical Infrastructure Protection Board, and tasked them with developing a strategy to secure cyberspace. Released in October 2002, the National Strategy to Secure Cyberspace "breaks out into a series of recommendations for cyberspace security at each of five levels: home users and small business, large enterprises, critical sectors, national issues, and global issues."[109] It identifies three strategic objectives: "prevent cyber-attacks against America's critical infrastructures; reduce national vulnerability to cyber-attacks; and minimize damage and recovery time from cyber-attacks that do occur."[110]

While a national strategy concerning computer network security is both necessary and timely, this document never establishes a hard policy, standards, regulations, or legal ramifications. Instead, "the National Strategy … recommends that industry and individuals simply take greater care."[111] If the government truly wants to place its hand into cyberspace and take on a greater role as an Internet protector, defender, and legal enforcer; then it needs to establish clear guidelines, regulations, standards, and legal ramifications. Mere suggestions will do little in the way of protecting the common user,

[109] Seth Ross, "Defending the National Strategy to Secure Cyberspace," *Securius Newsletter*, Volume 3 Number 3, November 18, 2002, http://www.securius.com, last accessed in May 2005.

[110] Michael T. Zimmer, "The Tensions of Securing Cyberspace: the Internet, State Power, and the *National Strategy to Secure Cyberspace*," *First Monday*, Volume 9, Number 3, March 2004, http://firstmonday.org/issues/issue9_3/zimmer/index.html, last accessed in May 2005.

[111] Ibid.

businesses, academia, and government institutions from cybercrime. Regardless of whatever action the government decides to take, a major concern that will remain is the protection of civil liberties of Internet users. The more the government extends its hand into cyberspace security, the more its opponents will tout the civil liberty card. Cyberspace security is a double-edged sword: the need to protect our infrastructure, privacy, economy – national security vs. the protection of our basic rights and liberties.

In the author’s opinion, the National Strategy to Secure Cyberspace is lacking in substance. The author acknowledges that the onus to protect networks falls on individual users and industry; however, if the government is going to tout a “national strategy” regarding cyberspace security, then it must take a more active role in establishing standards and regulations, training, and legal ramifications. Unfortunately, the very nature of the Internet runs counter to that of nation-states, which possess clear borders, laws, policies, and the ability to seek retribution. The one suggestion this strategy does espouse that may prove an asset in future cyberspace security is that of the “powerful incentive of insurance.” Since money rules the world and is the very essence of our capitalist society, much accountability for Internet and network security could be achieved through insurance policies. Only the future will tell what is in store for cyberspace security and the role the U.S. government will play in protecting our national security against cybercrime.

Future research in this field could include an analysis of classified information, to include security threat assessments, Israel’s CNO capabilities, and Palestinian CNO capabilities; discussion and analysis of legal issues regarding the use of offensive and defensive CNO, and a thorough discussion and analysis of the U.S.’s policies regarding offensive and defensive CNO.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

(listed in chronological order)

Sobelman, Ariel T. "An Information Revolution in the Middle East?." Strategic Assessment Vol. 1, No. 2 (1998). 05 May 2005 http://www.tau.ac.il/jcss/sa/v1n2p4_n.html.

"Israeli-Arab Warfare, Web-Style." Reuters 20 October 2000. 20 October 2000 http://www.wired.com/news/politics/0,1283,39587,00.html.

Wander, Josh. "MK Eitan Calls for Internet Truce." The Jerusalem Post 24 October 2000. 26 October 2000 http://www.jpost.com/Editions/2000/10/24/LatestNews/LatestNews.14275.html.

"Cyberwar Also Rages in Mideast." Associated Press 26 October 2000. 24 May 2005 http://www.wired.com/news/politics/0,1283,39766,00.html.

Venzke, Ben N. "Cyber Skirmish in the Middle East." iDEFENSE Intelligence Services 26 October 2000. 26 October 2000 http://www.idefense.com.

Hockstader, Lee. "Pings and E-Arrows Fly in Mideast Cyber-War." Washington Post Foreign Service 27 October 2000. 30 October 2000 http://washingtonpost.com

Kraft, Dina. "Israeli Web Sites Crash." The Associated Press 26 October 2000. 01 November 2000.

Nass, Gilad. "Hizballah Aims Electronic Warfare At Israel." Newsbytes 26 October 2000 LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

Salhani, Claude. "Commentary: Hezbollah Hackers Launch "Virtual Intifada"." United Press International 27 October 2000 LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

Kalman, Matthew. "Israeli-Palestinian Conflict Carries Over to Cyberspace." USA Today 27 October 2000 LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

Irvine, Jerry. "iDEFENSE: Middle East Tensions Move Online; Pro-Israeli and Pro-Palestinian Hackers Taking Down Web Sites, Threatening to Escalate Cyber War Tactics." Business Wire 31 October 2000 LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

"Abd-Rabbuh Says Israel Launching "Psychological Warfare" Against Palestinians." BBC Monitoring Middle East - Political 01 November 2000 LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

Walters, Lou, and Fionnuala Sweeney."Crisis in the Middle EAst: Israeli, Palestinian Hackers Incite War of Words in Cyberspace." CNN Today. CNN, Jerusalem. 02 November 2000. Broadcast. 26 April 2005 www.fdch.com.

Lev, Izhar. "E-Intifada: Political Disputes Cast Shadows in Cyberspace." Jane's Intelligence Review 03 November 2000. 18 August 2005 http://www.janes.com/security/international_security/news/jir/jir001103_1_n.shtml.

"Analysis: Israeli-Arab Cyber-Warfare." BBC Monitoring Research 03 November 2000. 03 November 2000 http://www.antionline.com/2000/11/02/MMED/0000-1456-KEYWORD.Missing.html.

Venzke, Ben N. "New Developments in Israeli-Palestinian Cyber Conflict." iDEFENSE Intelligence Services 04 November 2000. 04 November 2000 http://www.idefense.com.

"Hacking of Israeli Sites Continues - Israeli Hackers Jam Iranian Sites." The Jerusalem Post 06 November 2000. 07 November 2000 http://jpcost.com.

Disabatino, Jennifer. "Pro-Israel Web Site Hacked by Pro-Palestinian Cracker." Network World 06 November 2000 LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://www.nex.com.

Yehia, Ranwa. "Hackers Launch Phase Three of Online Intifada." The Daily Star 06 November 2000. 06 November 2000 http://www.dailystar.com.lb/04_11_00/art4.html.

Gentile, Carmen J. . "Hacker War Rages in Holy Land." Wired News 08 November 2000. 24 May 2005 http://www.wired.com/news/politics/0,1283,40030,00.html.

Machlis, Avi. "A Hacker With a Cause." The Standard 09 November 2000. 17 November 2000 http://www.TheStandard.com.

Schwartz, John. "When Point and Shoot Becomes Point and Click." The New York Times on the Web 12 November 2000. 12 November 2000 http://www.nytimes.com.

"Who's Winning the Arab-Israeli Cyber War?." Middle East News Online 15 November 2000. 17 November 2000 http://MiddleEastWire.com.

Gentile, Carmen J. "Israeli Hackers Vow to Defend." Wired News 15 November 2000. 24 May 2005 http://wired-vig.wired.com/news/print/0,1294,40187,00.html.

Mishmari, Aviva. "Hacking for Israel." C4I.org. 15 November 2000. C4I.org. 17 November 2000 http://www.c4i.org.

"Mideast Attacks Extend to Internet Web Sites." The Jerusalem Post 16 November 2000. 20 November 2000 www.jpost.com.

Heller, Jeffrey. "Fake Israeli Army Web Site Goes on Offensive." Reuters 16 November 2000. 17 November 2000.

Krebs, Brian. "Hackers Worldwide Fan Flames in Middle East Conflict." ComputerUser.com 25 November 2000. 12 August 2005 http://computeruser.com/clickit/printout/nes/337149000003309440.html.

Maxwell, Bill. "Middle East War Rages on the Internet." St. Petersburg Times 30 November 2000. 01 December 2000 http://web.lexi-nexis.com.

http://www.attrition.org/mirror/attrition/2000/11/04/www.cognifit.co.il.

Whitaker, Brian. "War Games On the Net: But This Time It's for Real." The Guardian Unlimited 30 November 2000. 24 May 2005 http://www.guardian.co.uk/.

Gentile, Carmen J. "Palestinian Crackers Share Bugs." Wired News 02 December 2000. 11 August 2005 http://www.wired.com/news/print/0,1294,40449,00html.

Shreve, Jenn. "Covering the Middle East, Web Style." The Industry Standard 05 December 2000. 05 December 2000 http://www.idgnews.net.

Nelson, Cletus. "Hackers Holy Wars." Disinformation. 19 December 2000. Disinformation. 14 July 2005 http://www.disinfo.com.

"Israeli-Palestinian Cyber Conflict (IPCC) Version 2.0 Public Release." iDEFENSE Intelligence Services Report January 2001: 01-80.

"Israel and Palestine Step Up Cyberwar." RIA Novosti 05 January 2001 LexisNexis. Nexis.com. The Dudley Know Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

Hershman, Tania. "Israel's Seminar on Cyberwar." Wired News. 10 January 2001. Wired News. 26 May. 2005 http://www.wired.com/news/politics/0,1283,41048,00.html.

Galvin, John. "The Real Online Battleground: There's Another World War Brewing, and Most of Us Don't Even Know It." ZdNet News 07 February 2001. 02 February 2001 http://www.zdnet.com/.

Daly, John C. "Analysis: The Virtual Intifada." United Press International 24 April 2001 LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

Lemos, Robert. "Little Damage Done by Pro-Palestinian Virus." CNET News.com. 19 March 2001. CNET News. 20 March 2001 http://news.cnet.com.

Markowitz, Elliot. "The New World of Terrorism." Tech TV. 08 March 2001. Tech TV. 08 March 2001 http://www.techtv.com.

Lawson, Sean. "The Cyber-Intifada: Activism, Hactivism, and Cyber-Terrorism in the Context of the "New Terrorism"." Online posting. 2001. Prepared as a Seminar Paper for the Course, Information Warfare and Security, taught by Dorothy Denning, Georgetown University, Fall 2001. 14 July 2005. http://www.rpi.edu/lawsos/Cyber-intifada.pdf

McLaughlin, W. Sean. "E-Intifada: Internet in the Palestinian Uprising." Foundations 2001: 33-54.

"Israel Under Hack Attack." Information Warfare Monitor. 16 April 2002. Information Warfare Monitor. 28 August 2005 http://www.infowar-monitor.net.

Trendle, Giles. "Internet Warfare in the Middle East." The World Today April 2002: Vol. 58. :7-8. Royal Institute of International Affairs. ProQuest. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://libprox..nps.navy.mil/login?url=http://proquest.umi.com/pqdweb?did=112885407&Fmt=4&clientld=11969&RQT=309&VName=PQD.

Trendle, Giles. "Cyberwars: The Coming Arab E-Jihad." Middle East April 2002:5-8. ProQuest. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://libproxy.nps.navy.mil/login?url=http://proquest.umi.com/pqdweb?did=112931219&Fmt=4clientld=11969&RQT=309&VName=PQD.

Hoffman, Lisa. "Cyber-Wars Between Israel and Palestinians." Scripps Howard News Service 22 April 2002 LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

NIPC Daily Report, 19 June 2002.

"Pro-Islamic Hackers Join Forces." Online posting. 19 June 2002. Attrition.org. 24 June 2002. http://news.bbc.co.uk/hi/english/sci/tech/newsid_2052000/2052320.stml.

WFD. WFD (World's Fantabulous Defacers). 24 June 2002 http://www.dominasecurity.com/hackerz/wfd.html.

Mietkiewicz, Mark. "Israeli-Palestinian Conflict Entrenched in Cyberspace." New Jersey Jewish News 25 July 2002: Vol. LVI., No. 30:34. LexisNexis. Nexis.com. The Dudley Know Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

"Activists' Names Listed in Hackers' Terror E-mail." Overseas Security Advisory Council. 05 August 2002. Overseas Security Advisory Council. 09 August 2002 http://www.ds-osac.org/edb/cyber/news/story.cfm.

"Pro-Islamic Militant Hacker Groups Boost Attacks Security Company Says." The Jerusalem Post Internet Edition 01 October 2002. 04 October 2002 http://www.jpost.com

"Middle East Tension Fuels Hacker Fury - Q3 Worst Hit." mi2g Intelligence Briefing. 01 October 2002. mi2g. 04 October 2002 http://www.mi2g.net/cgi/mi2g/press/images/digital_attacks_year.pdf.

Hishmeh, George S. "Activists Under Cyber-Attack in Internet Propaganda." PM Watch. 10 February 2003. Palestine Media Watch. 18 August 2005 http://www.pmwatch.org/pmw/manager/features/display_message.asp?mid=594.

"An Assessment of Recent Pro-Islamic Hacking Activity and Future Prospects." iDEFENSE iALERT White Paper November 2002: 01-17.

Allen, Patrick D., and Chris C. Demchak. "The Palestinian-Israeli Cyberwar." Military Review 01 March 2003: Vol. 83. :52-59. LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 <http://www.nexis.com>.

"IDF Raids ISM Media Office, Others (ISM Press Release)." Information Warfare Monitor. 09 May. 2003. Information Warfare Monitor. 28 August 2005 http://www.infowar-monitor.net.

Ackerman, Gwen. "Israeli High Tech Targets U.S. Security Market." Information Warfare Monitor. 04 August 2003. Information Warfare Monitor. 28 August 2005 http://www.infowar-monitor.net.

"Mossad Recruiting Site Hacked." Information Warfare Monitor. 04 November 2003. Information Warfare Monitor. 28 August 2005 http://www.infowar-monitor.net.

Abbey, Alan D. . "Virtual Jihad." Information Warfare Monitor. 08 May. 2004. Information Warfare Monitor. 28 August 2005 http://www.infowar-monitor.net.

Glick, Caroline B. . "Information Warfare 101." The Jerusalem Post 16 July 2004:24- . LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

Amayreh, Khalid. "Israel to Wage Psychological Warfare." Information Warfare Monitor. 25 January 2005. Information Warfare Monitor. 24 May. 2005 http://infowar-monitor.net.

Isikoff, Michael, and Mark Hosenball. "Virtual Jihad." Newsweek 10 February 2005. 28 August 2005 http://www.msnbc.msn.com.

Saad, Hussein. "Hizbollah Flies Drove Over Northern Israel." Reuters 11 April 2005. 28 May 2005.

Amin, Hussein Y. "Social Engineering: Transnational Broadcasting and Its Impact on Peace in the Middle East." Global Media Journal Spring 2005. 03 May 2005 http://lass.calumet.purdue.edu.

Rashed, Dina. "Cyber War: The Civilians' War and Politics." IslamOnline.net. IslamOnline.net. 18 August 2005 http://www.islamonline.net/english/Politics/2000/1/Article17.shtml.

Lawson, Sean. The Cyber-Intifada Resource Guide. 12 August 2005 http://www.geocities.com/db8r.geo/.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

(listed in alphabetical order)

- a.israforce.net
- Hizballa - No More, at home.online.no/~oelpeleg/hiz.htm
- http://members.nana.co.il/planet/yair_n/index.htm
- Members.nana.co.il/planet/carmelb
- Mock Hezbollah Site, at www.hizballa.org
- SmallMistake, at smallmistake.welcome.to
- www.crashme.com [112]
- www.wizel.com

[112] iDEFENSE recommends against visiting this site because it attacks visitors' browsers.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C

(listed in alphabetical order)

- 195.138.224.2
- 207.222.197.194
- Al-Bawaba Portal site, at http://www.albawaba.com
- al-Manar, at http://www.almanar.com.lb
- al-Manar, at http://www.manartv.com
- Hafeez Center Global Internet Café, at http://www.hafeezcentre.com.pk
- Hamas, at Hamas.org
- Hezbollah, at Hezbollah.org
- Hezbollah, at Moqawama.org
- Hezbollah, at Nasrallah.net
- Hezbollah site, at http://www.hizbollah.org
- Iranian Foreign Ministry site, at http://mfa.gov.ir
- Iranian Ministry of Agriculture, at http://www.moa.or.ir
- Islam Web, at http://www.islamweb.net
- Islamic Republic News Agency, at http://www.irna.com
- Islamic Society of North America, at http://www.isna.net
- Islamic University, Gaza site, at http://www.iugaza.edu
- Khaleej.com, at http://www.khaleej.com
- Ministry of Awqaf and Islamic Affairs, Qatar site, at http://www.islam.gov.qa
- Palestine National Databank State Information Service, at http://www.sis.gov.ps
- Palestine-Info, at Palestine-info.net
- Palestinian National Authority, at http://www.pna.gov.ps
- Palestinian National Authority, at PNA.org
- Sakhr Software Co. site, at http://www.ajeeb.com

- Talk Islam, Library of Islamic Web Sites, at http://www.talkislam.com
- Ummah.net, at 212.240.0.12
- Ummah.net, at http://kano.virtual-pc.com
- Ummah.net, at Ummah.com
- Ummah.net, at Ummah.net
- Ummah.net, at Ummah.org
- United Arab Emirates Dept. of Civil Aviation site, at http://www.dcaauh.gov.ae
- webhosting.ajeeb.com
- www.primebank.com.pk

Pro-Israeli Tradecraft (listed in alphabetical order)

- .To (Free Web Referrals)
- Dreambook (Guestbook Service)
- Geocities.com (Free Web Hosting)
- Namezero.com (Free Web Hosting)
- Nana.co.il (Free Web Hosting)
- Surfree.net.il
- Yahoo! (Free Email)

APPENDIX D

(listed in alphabetical order)

- angelfire.com/oh4/irsa2000
- defend the Resistance, at members.tripod.com/irsa2001
- defend.unity-news.com/
- hizbollah.unity-news.com/
- irsa2000.jumpfun.com
- killisrael.arjika.com/arabic.htm
- resistance-defend.freeservers.com
- unity.vdirect.com
- www.bahraingate.8k.com
- www.fightisrael.com
- www.freespeech.org/unity-nes/defend
- www.ummah.net/unity/defend

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E

(listed in alphabetical order)

- http://pub23.ezboard.com/fbaderonlinefrm13
- http://quds.gq.nu/killisrael.htm
- http://unity-news.org
- http://www.almuhajiroun.com
- http://www.fightisrael.com

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F

(listed in alphabetical order)

- ABIS site, at http://www.asbis.sk
- Achva Academic College's E-learning, at http://online.achva.ac.il
- albert.ph.biu.ac.il
- Al-Libaas Accessories site, at http://www.al-libaas.com
- All-Kosher Index, at http://www.kosher.co.il
- American Israel Public Affairs Committee, at http://www.aipac.org
- AMTEL Slovensko Ltd. Site, at http://www.amtel.sk
- Anti-Defamation League (ADL), at http://www.adl.org
- Ardom Telecomputing of Israel, at http://www.ardom.co.il
- ARON site, at http://www.aron.be
- AT&T Corp., at http://www.att.com
- Bank of Israel, at http://www.bankisrael.gov.il (161.58.232.244)
- Bayan Systems, at http://www.bayan.co.il
- Borha Torah, at http://www.borhatorah.org
- BSNL Nagpur (Depart of Telecom) site, at http://nagpur.dotindia.com
- Cairo University, at http://www.cairo.eun.eg
- Caspit Ltd., at http://www.caspit.co.il
- Central Florida Bankruptcy Law Association site, at http://www.cfbla.org
- Christian Sharing Center site, at http://www.christiansharing.org
- Cognifit Ltd., at http://www.cognifit.co.il
- Compact Studio site, at http://www.dvdbest.sk
- Comsec Group Ltd., at http://www.comsec.co.il (194.90.202.39)
- Comune di Scandiano, at http://www.comune.scandiano.re.it
- Corporacion Peruana de Aeropuertos y Aviacion Comercial S.A. site, at

- http://www.corpac.gob.pe
- Cowboys Orlando Night Club site, at http://www.cowboysorlando.com
- Cursos de Bolsa site, at http://www.cursobolsa.com
- CVD Data Services, at http://lab.cvdds.com
- delhinms.mtnl.net.in
- Deutsche Forschungsanstalt fuer Luft – und Raumfahrt e.V. (DLR) site, at
- http://www.weblab.dlr.de
- Dilim Site, at http://www.dilim.co.il
- Dizasta Productions site, at http://www.dizasta.net
- dns0.whuci.edu.cn
- Ebrick Inc., at http://lotus.ebrick.com
- Efrat DSP Group, at http://www.efratdsp.co.il
- EgyNile ISP, at http://egynile.com
- Elgev Electronics, at http://www.elgev.co.il
- Forma, Ltd. Site, at http://www.deiure.sk
- Frostbit.com, at http://www.frostbit.com
- Gega Net ISP, at http://dev.gega.net
- Gilo High School, at http://www.gilo.jlm.k12.il
- Golden Lines, at http://www.goldenlines.co.il (212.117.129.81)
- Gvanim Financim, Kibutz Shefayim Israel, at http://www.gvanim.co.il
- Health Infosystems Association, Israel, at http://www.healthinfonet.co.il
- Hebrew University of Jerusalem, Israel site, at http://daat.ls.huji.ac.il
- Hebrew University of Jerusalem, Israel site, at http://www.music.md.huji.ac.il
- Hed-Arzi, at http://www.hed-arzi.co.il
- Indian Institute of Science Dept. of Mechanical Engineering site, at
- http://mecheng.iisc.ernet.in
- Indian Institute of Science Dept. of Metallurgy, at http://www.metalrg.iisc.ernet.in
- Indian Institute of Science Materials Research Center site, at http://arun.mrc.iisc.ernet.in

- Indian Institute of Science Solid State and Structural Chemistry Unit, at http://zeolite.sscu.iisc.ernet.in
- Israel.com, at http://www.israel.com (63.194.226.226)
- Israeli Academic, at http://www.yvc.ac.il
- Israeli Academic Sub-Domain, at http://www.netanya.ac.il
- Israeli Air Force, at http://www.iaf.org.il
- Israeli Defense Forces (IDF), at http://www.idf.il (192.117.1.1 and 212.14.3.30.101)
- Israeli Foreign Ministry, at http://www.mof.gov.il
- Israeli Government, at http://www.israel.org (194.90.246.13 and 212.143.236.4)
- Israeli Government Site (147.237.72.20)
- Israeli Knesset
- Israeli Ministry of Defense, at http://www.mod.gov.il
- Israeli Ministry of Interior, at http://www.moin.gov.il
- Israeli Ministry of National Infrastructures, at http://www.mni.gov.il
- Israeli National Police, at http://www.police.gov.il
- Israeli Prime Minister's Office, at http://www.pmo.gov.il (147.237.72.93)
- Jen Communications, at http://www.jen.co.il
- Jerusalem Books, at http://www.jerusalembooks.com
- Jerusalem Post, at http://www.jpost.com
- Jewish Bible Association, at http://www.jewishbible.org
- JMJ Internet Services, at http://www.jmjservices.com
- KAIZ site, at http://www.kaiz.com
- Karnataka Telecom Circle site, at http://www.karnataka.dotindia.com
- KIS Technologies, at http://www.kisnet.co.il
- Kolhapur Telecom District site, at http://www.kolhapur.dotindia.com
- Kuala Lumpur Department of Urban Transportation site, at http://www.jpbdbkl.gov.my
- La Cruz Azul de Puerto Rico Inc. site, at http://www.cruzazul.com.mx

- Lal Bahadur Shastri National Academy of Administration, Mussoorie, at http://www.lbsnaa.ernet.in
- Lantronics Computer Networking Ltd., at http://www.lantronics.co.il
- Los Alamos Neutron Science Center site, at http://www.lansce.lanl.gov
- Lucent Technologies, at http://www.lucent.com (192.11.229.2)
- Lymphedema Awareness Foundation site, at http://www.lymphaware.org
- mail.topnet.co.il
- Malaysian Rubber Board site, at http://www.lgm.gov.my
- MBA International School of Business Administration Management, at http://www.eiba.biu.ac.il

  MBA International School of Business Administration Management, at http://www.mba.biu.ac.il
- Merical (IN), at http://email.merical.ac.in
- modiin.haifa.ac.il
- National Centre for Radio Astrophysics site, at http://sakthi.ncra.tifr.res.in
- NB a.s. site, at http://www.nbas.cz
- Netanya Academic College, at http://mars.netanya.ac.il
- NetVision
- Open University-Jerusalem, at http://www.jccopenu.ac.il
- Order in a Click, at http://www.order-click.co.il
- Ornetix, at http://ntserver.ornetix.co.il
- Partners in Torah, at http://www.partnersintorah.org
- PC Center, at http://www.pc-center.co.il
- Pelenews site, at http://www.pelenews.co.il
- Pf1 Systems Ltd., at http://www.pf1.co.il
- Phillips Community College-University of Arkansas site, at http://www.pccua.cc.ar.us
- Pirchei Shoshanim, at http://www.pirchei.co.il
- Qatar Ministry of Awqaf and Islamic Affairs, at http://www.islam.gov.qa

- Rabia Gupta Design site, at http://www.styletantra.com
- Radwiz, at http://www.radwiz.co.il
- Retirement Living Management site, at http://www.retliv.com
- Rooster, at http://mail.rooster.co.il
- Rotter.net, at http://www.rotter.net (194.90.202.20)
- Scicom site, at http://www.scicom.com.my
- Server Computers site, at http://www.netserver.co.il
- sgl1.lanres.com
- Shavatz High School, at http://www.savatz.givataim.k12.il
- Shema Yisrael Torah Network, at http://shemayisrael.co.il
- Shenkar College at http://www.shenkar.ac.il
- Shop.chemolak.sk
- Sira1.sira.it
- Sivan-North Computer, at http://www.sivan-north.co.il
- SofTech Tecnologia em Informatica LTDA, at http://www.stn.com.br
- Solski Center PTUJ site, at http://www.s-scptuj.mb.edus.si
- SOMA Galleries, at http://www.somagalleries.com
- Tahal Group, at http://www.tahal.co.il
- Tel Aviv Chamber of Commerce, at http://www.chamber.org.il
- Tel Aviv Stock Exchange, at http://www.tase.co.il (192.116.46.129)
- Temple Mount in Jerusalem at http//www.templemount.org (216.10.100.29)
- Terminal-Computers & Multimedia, at http://www.terminal.co.il
- The American University in Cairo, at http://www.aucegypt.edu/hi.html
- The Temple Institute, at http://www.templeinstitute.org (161.58.226.14)
- The Ultimate Shabbat Site, at http://www.shabat.co.il
- topcom.topnet.co.il
- Torah Educator, at http://www.toraheducator.org
- United Studios Corp., at http://www.usidentity.com
- University of Oklahoma Administration site, at http://admin-scb.ouhsc.edu

- University Medical Center Nijmegen Dept. of Urology, Netherlands site, at http://uroworld.azn.nl
- University of Chicago Computer Science Dept. site, at http://hamachi.cs.uchicago.edu/
- Visiting Israel Students Association, at http://www.visa.org.il
- VOLasia limited site, at http://www.volasia.com
- Watersports World, at http://www.watersportsworld.com
- Web of India site, at http://dmss.webindia.com
- Web of India site, at http://servlet.webindia.com
- Web of India site, at http://servlet2.keralatourism.org
- Web of India site, at http://tanishq.webindia.com
- Web of India site, at http://webmail.webindia.com
- WebStyle Internet Solutions, at http://www.webstyle2000.com (207.159.139.113)
- Western-Galilee College, at http://wgalil.ac.il
- Wisconsin K12 Schools site, at http://www.sharon.k12.wi.us
- Wizel.com, at http://www.wizel.com (64.33.48.76)
- World Peace Center, at http://www.worldpeacecenter.org
- www.ann-arbor.med.va.gov
- www.arttalk.com
- www.aztek.co.il
- www.cardcentrum.sk
- www.carroll.k12.ga.us
- www.cog.co.jp
- www.dol.wa.gov
- www.files4u.co.il (same as www.karate.org.il)
- www.hmcnet.com
- www.infinity.com.eg
- www.microconnectors.com

- www.pryor.k12.ok.us
- www.robotec.co.il
- www.scjh.kh.edu.tw
- www.stadtklima.de
- www.syscom.co.il
- www.topnet.co.il
- www.whuci.edu.cn
- www.xmlprobe.com
- www3.co.oakland.mi.us
- Yizrael Valley College (Mihlelet Emek Yizrael), at http://www.yvc.ac.il
- Zefat Regional College, at http://www.zrc.ac.il

Pro-Palestinian Tradecraft (listed in alphabetical order)

- Angelfire (Free Web Hosting)
- eGroups (Free List Hosting)
- GeoCities (Free Web Hosting)
- Homestead.com (Free Web Hosting)
- Hotmail.com (Free Email)
- Hushmail.com (Free Secure Email)
- Jumpfun.com (Free Web Hosting)
- ListBot (Free List Hosting)
- Tripod.com (Free Web Hosting)
- Ummah.net (Web Hosting)
- Xdrive.com (Free File Sharing)
- Yahoo! (Free email)

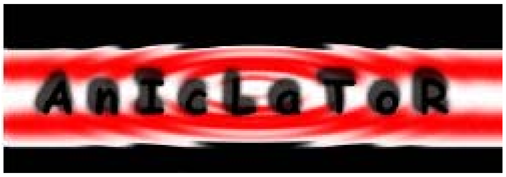
THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G

(listed in alphabetical order)

1. Other Actors

- **AnIcLaToR**: AnIcLaToR is responsible for the first defacement of a U.S. government Web site since this Palestinian-Israeli cyber conflict began. AnIcLaToR defaced the site at mrdata.usgs.gov. Rather than supporting one side of the conflict, this attacker advocated an end to the Israeli-Palestinian ground conflict altogether. AnIcLaToR’s work appeared to be non-destructive in nature. AnIcLaTor is believed to be based in Brazil. On November 7, 2000, AnIcLaToR defaced the SofTech Tecnologia em Informatica LTDA site, at www.stn.com.br. AnIcLaToR is a member of prime suspectz.



- **DeTH ‘Sauron**: This group includes DeTH Crew or DeTH Brotherhood, and members include: DeTH`Watice, DeTH`Flameboy, DeTH`Angelus, DeTH`Arcrass, DeTH`Milenko, DeTH`Altered, DeTH`Digital, DeTH`Monarch, DeTH`Romeo, DeTH`Overide, DeTH`Xanor, Star/Yung/Yungsta, and Havokator. On November 1, 2000, DeTH ‘Sauron defaced the web site of the Jarvis Entertainment Group, at http://www.gamingrevolution.com. The site was overwritten with a message regarding the Israeli-Palestinian conflict, deriding both sides: “Not many people realise the severity of the constant religious warfare and other CRAP that goes on in the middle east between Jews and arabs.” According to DeTH ‘Sauron, the site was backed up as index1.html and nothing on the site was damaged.

2. Other Targeted Sites (listed in alphabetical order)

- Hebrew University of Jerusalem, Israel, at http://shemesh.fiz.huji.ac.il
- Jarvis Entertainment Group, at http://www.gamingrevolution.com
- Sheffield Hallam University site, at jeff.sci.shu.ac.uk
- US Geological Survey’s Mineral Resources Online Spatial Data, at http://mrdata.usgs.gov
- www.as.huji.ac.il

THIS PAGE INTENTIONALLY LEFT BLANK

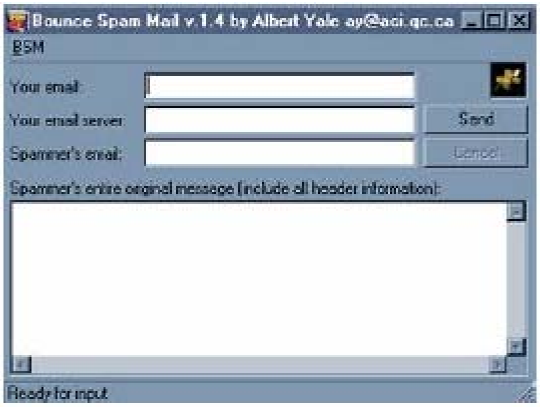
APPENDIX H

(listed in alphabetical order)

- **ahlizevil aka evilping**: Attack tool distributed by pro-Palestinian attackers. It is believed to be the same as evilping.

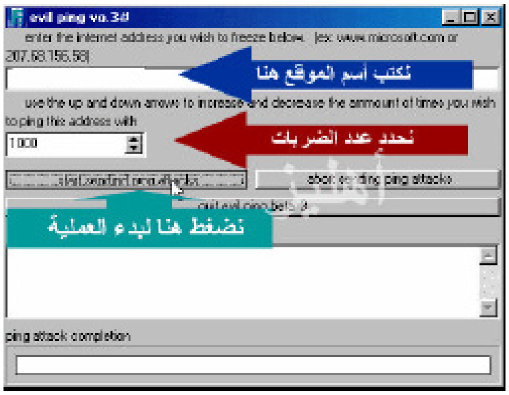
- **Attack 2.41 and Attack 2.51**: Attack versions 2.41 and 2.51 were used by the Palestinians to conduct three different types of assault: ping attacks, HTTP GET requests, and Web attacks. All three can be used at the same time. The difference between 2.41 and 2.51 seems to be minor bug fixes.

- **Bounce Spam Mail v1.4**: Email attack tool distributed by pro-Palestinian attackers.


Bounce Spam Mail v.1.4 by Albert Yale ay@aci.qc.ca
BSM
Your email:
Your email server:
Spammer's email:
Send
Cancel
Spammer's entire original message (include all header information):
Ready for input

- **defend**: A FloodNet-type tool known as “defend” was used by a number of pro-Palestinian groups to attack at least seven different targets. At least three different versions of the tool are known to be in existence, each successive version that added additional sites to defend’s target list. The tool is simple in nature, but required several attackers to be effective. It used a new method of defeating caching problems experienced by cyber activists in the past. During an attack, defend requests non-existent pages on targeted sites by calling for URLs based on the current date and time. The pro-Palestinians have mirrored the attack tool on Angelfire.com, Tripod.com, Ummah.net, and Jumpfun.com hosting sites.

- **evilping (07/98 release & 11/99 release), a.k.a. ahlizevil**: Attack tool distributed by pro-Palestinian attackers.



enter the internet address you wish to freeze below. (ex: www.microsoft.com or 207.68.156.58)

نكتب أسم الموقع هنا

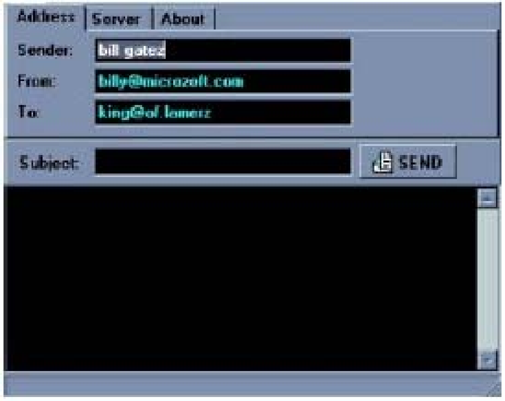
use the up and down arrows to increase and decrease the ammount of times you wish to ping this address with

1000

نحدد عدد الضربات

نضغط هنا لبدء العملية

- **FakeMail**: Email attack tool distributed by the pro-Palestinians.



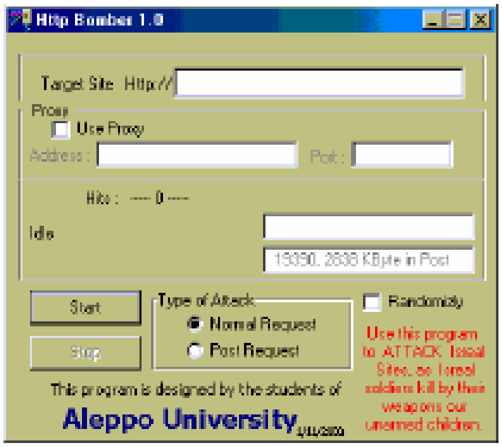
Sender: bill gatez

From: billy@microzoft.com

To: king@of.lamerz

Subject:

- **HTTP Bomber 1.0**: Pro-Palestinians used a tool called HTTP Bomber. The tool was distributed on www.kuds.8k.com, which was taken offline in early November 2000. With its very simple user interface, Bomber appears to have allowed a user to target specific Web sites either by its URL or IP address. The attack tool claimed to generate numerous HTTP GET and POST requests. In addition, the attacker has the option of letting the tool randomly implement either of the two attacks.



Target Site Http://

Proxy

□ Use Proxy

Address :   Port :

Hits : ---- 0 ----

Idle

15350, 2838 KByte in Post

Type of Attack

● Normal Request

○ Post Request

□ Randomly

Use this program to ATTACK Isreal Sites, as Isreal soldiers kill by their weapons our unarmed children.

This program is designed by the students of

Aleppo University 1/11/2000

- **HTTP Bomber 1.001b**: Distributed on www.kuds.8m.com, it is believed to have gone into circulation on November 7, 2000. The graphical user interface (GUI) appears to have been identical to HTTP Bomber 1.0.

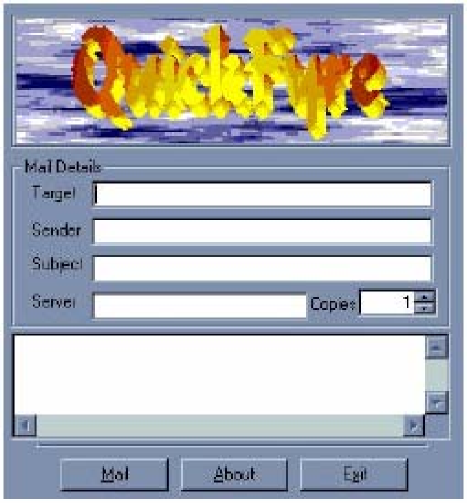
- **Injustice**: On March 20, 2001, Palestinians sent "Injustice," a mass mailing computer virus with a worm that is a Visual Basic script attachment called INJUSTICE.TXT.VBS. The virus appeared as an attachment to an e-mail message with the subject line "RE: Injustice"; once opened, the program displayed an anti-Israeli message in a text dialog box. "PLEASE ACCEPT MY APOLOGIES FOR DISTURBING YOU," states the message. "Rembmer that one day YOU may be in this situation. We need every possible help." The rest of the message described the death of a 12-year-old Palestinian boy. The virus sent itself in e-mail messages to the first 50 entries in the infected computer's Outlook address book, along with 18 Issraeli government addresses, 8 organizations, and to the Webmaster of Israel's official Web site. "Injustice" used Microsoft's Internet Explorer to open six windows to a variety of Web sites, including an electronic petition to the United Nations High Commissioner for Human Rights.

- **juno**: A SYN flood tool.

- **Ping Attack**: U.S. university students were asked to attack pro-Palestinian Web sites. iDEFENSE confirmed that posts on listservs belonging to at least one prominent American university gave students directions for launching ping floods against prominent Palestinian targets. These emails also circulated (with unknown prevalence) to members of the public. The following provide examples of Web sites targeted: Hezbollah, Hezbollah Secretary General Sayyed Hassan Nasrallah, Hezbollah's al-Manar Television, Hamas, the Hamas-supported Palestinian Information Center, Hezbollah's Islamic Resistance Support Association, and the Palestinian National Authority.

- **Ping of Death**: The Ping of Death used a utility to create an IP packet that exceeded the maximum size allowed by the IP specification. The oversize packet was then sent to an unsuspecting system. The use of this maliciously crafted packet may cause systems to crash, hang, or reboot. This attack tool was not new to the arsenal of cyberweapons during the Palestinian-Israeli Cyberconflict. As a source of defense, operating systems and some Layer 3 communications hardware can be configured to filter out oversize packets, thus preventing a ping of death.

- **QuickFyre**: Email attack tool, distributed by pro-Palestinian attackers, capable of generating more than 32,000 messages to a targeted address with a single click.



- **Shell Script by dodi**: iDEFENSE examined a portion of shell code that was posted on the COGNIFIT defacement. Preliminary analysis of the code indicated that, if placed onto a Linux or Unix system, the code would delete essentially all files on the computer with the exception of the OS at a specified time. It would then execute an attack tool, if it is located in the local directory, and begin to attack a targeted site. The code examined by iDEFENSE executed the "juno" SYN flooder and began an attack against the www.idf.il site on port 80. This tool could easily be modified to target any site the attacker wished. It is reasonable to suspect that dodi and other attackers may have installed such code on previously defaced or compromised sites. Organizations whose sites have been targeted or are victims of attacks connected to the Palestinian-Israeli Cyberconflict were advised to immediately begin searching for a file called "isat." Companies were also advised to examine all "cron" and "at" jobs to see if anything unusual was scheduled to run.

- **slice**: A SYN flood tool.

- **Smurf attacks**: Smurf attacks are an early variation of a ping attack. The Smurf attack exploits misconfigured networks to reply to a ping sent to a network broadcast address. By sending one packet, an attacker can trigger hundreds of packets to bounce back in reply. The use of these attacks raised awareness of this misconfiguration. Most administrators have since fixed the problem. With the number of viable Smurfing targets reduced, many hackers turned to denial-of-service attacks that involved compromising a number of hosts and manually sending floods against a target. This required hackers to log into each of these machines individually, resulting in a timeconsuming process. In response, hackers and security experts began to develop new DDoS tools. These tools were designed to speed up DDoS attacks by automating the process. These tools still required an intruder to penetrate each host and load the slave server; however, with the tools, this need only be done once. As a result, a machine designated as the "master" of the network could be used to communicate with all of the "slaves," and command them to launch the packet flood at the appropriate moment.

- **WinSmurf**: Attack tool distributed by the pro-Israeli group Hackers of Israel Unite and pro-Palestinian attackers. Hackers of Israel Unite claimed to have successfully downed an Arab site using this tool over a 56K dial-up connection and one ADSL line.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allen, Patrick D. and Chris C. Demchak. "The Palestinian-Israeli Cyberwar." Military Review 01 March 2003: 83, 52. LexisNexis. Nexis.com. The Dudley Knox Library at the Naval Postgraduate School. 26 April 2005 http://www.nexis.com.

Anderson, Paul. "Cyber-Jihad Reportedly Enters Phase III...." Daily Star 05 November 2000. 05 November 2000 http://www.dailystar.com.lb/04_11_00/art4.htm

Armstrong, Helen and John Davey. "Educational Exercises in Information Warfare - Information Plunder and Pillage." 5th National Colloquium for Information Systems Security Education. George Mason University, Fairfax. 22 May 2001.

Arquilla, John and David Ronfeldt. “Afterword (September2001): The Sharpening Fight for the Future,” in Networks and Netwars: The Future of Terror, Crime, and Militancy. Online posting. 2001. Rand. May 2005. www.rand.org/publications/MR/MR1382.

Arquilla, John and David Ronfeldt. “The Advent of Netwar (Revisited),” in Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND, 2001: 1-25, http://www.rand.org/publications/MR/MR1382/MR1382.ch1.pdf.

Arquilla, John. "The Great Cyberwar of 2002." Wired Magazine February 1998. 11 August 2005 http://hotwired.wired.com/collections/future_of_war/6.02_cyberwar_2002.pr.html .

Arquilla, John , and David Ronfeldt. "Cyberwar is Coming!." Comparative Strategy, Vol. 12, no. 2, 1993: 141-165.

Beitler, Ruth M. The Path to Mass Rebellion: An Analysis of Two Intifadas. New York: Lexington Books, 2004.

Berkowitz, Bruce. "Information Warfare: Time to Prepare." Issues in Science and Technology online, Winter 2000. 12 August 2005 http://www.issues.org/issues/17.2/berkowitz.htm.

Blank, Stephen J. "Rethinking Asymmetric Threats." Strategic Studies Institute. September 2003. 23 May 2005 http://www.carlisle.army.mil/ssi/.

Bunt, Gary R. Virtually Islamic: Computer-mediated Communicaton and Cyber Islamic Environments. Cardiff: University of Wales Press, 2000.

Cordesman, Anthony H. "Forging a Transatlantic Strategy for Terrorism and Asymmetric Warfare." Center for Strategic and International Studies January 2002.

"Country Profile: Israel and Palestinian Territories." BBC News. 07 July 2005. 27 August 2005 http://newsvote.bbc.co.uk/go/pr/fr/-/2/hi/middle_east/country_profiles/803257.stm.

Davies, Catriona. "U.S. Army Computers 'Shut Down by Hacker' ." news.telegraph 28 July 2005. 11 August 2005 http://news.telegraph.co.uk/news/main.jhtml?xml=/news/2005/07/28/nhack28.xml

Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." IWS - The Information Warfare Site. Nautilus Institute. 27 August 2005 http://www.iwar.org.uk/cyberterror/resources/denning.htm.

Denning, Dorothy E. "Cyberterrorism." Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives 23 May 2000. 27 August 2005 http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Denning, Dorothy E. “Is Cyber Terror Next?” in Understanding September 11. New Press: 2002.

Elmusharaf, Mudawi M. "Cyber Terrorism: The New Kind of Terrorism." Computer Crime Research Center. 08 April 2004. Computer Crime Research Center. 18 August 2005 http://www.crime-research.org/articles/Cyber_Terrorism_new_kinds_Terrorism.

Emerson, Steven. American Jihad: The Terrorists Living Among Us. New York: The Free Press, 2002.

Giacomello, Giampiero. "Measuring 'Digital War': Learning from the Experience of Peace Research and Arms Control." Infocon Magazine October 2003. 23 May 2005 http://www.iwar.org.uk/infocon/.

Guisnel, Jean. Cyberwars: Espionage on the Internet. Cambridge: Perseus Books, 1997.

"Hackers Target County's Retirement Plan." 10news.com 31 July 2005. 24 August 2005 http://intel.socom.smil.mil/sociic/osec/weekly/05/0508/050805/050805iw07.htm

Hawkins, Charles F. "Coming to Grips with Information Warfare: A Western Perspective." Beijing Special Lecture. China Defense Science & Technology Center, Beijing. March 1997.

Hildreth, Steven A. "Cyberwarfare." CRS Report for Congress 19 June 2001. 23 May 2005 http://www.fas.org/irp/crs/RL30735.pdf.

"Information Operations." IWS - The Information Warfare Site. February 2004. Canadian Security Intelligence Service. 11 August 2005 http://www.iwar.org.uk/iwar/resources/canada/infoops.htm.

Jones, Andy, Gerald L. Kovacich, and Perry G. Luzwick. "Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part 1." Information Systems Security September/October 2002: 09-20.

Kirk, Michael and Jim Gilmore. "Cyber War!." Frontline. PBS. 24 April 2003. Transcript. 12 August 2005 http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html.

Lancaster, John. "Abroad at Home: Mideast Hacker Wars Hit U.S. Group's Site." The Washington Post 03 November 2000. 23 May 2005 http://washingtonpost.com

Lancaster, John. "The Cyberwars of the Middle East Have Spread to Washington." The Washington Post 03 November 2000. 03 November 2000 http://washingtonpost.com/wp-dyn/articles/A4288-2000Nov2.html

Lawrence, Stacy. "Terrorism and the Internet." Technology Review February 2005: Vol. 108, 50-51. Student Resource Center. Student Resource Center. Brandon High School Library, FL. 19 August 2005

Lemos, Robert. "The New Age of Hacktivism." ZDNN 08 November 2000. 08 November 2000 http://www.zdnet.com/zdnn/stories/news/0,4586,2651320,00.html

Luening, Erich. "Lucent Says Mideast Hackers Attacked Web Site." c|net News.com 02 November 2000. 18 August 2005 http://news.com.com/2102-1017_3-248056.html

Markoff, John. "Cyberwarfare Breaks the Rules of Military Engagement." The New York Times on the Web 17 October 1999. 12 August 2005 http://www.nytimes.com/library/review/101799cyberwarfare-review.html

Messmer, Ellen. "Threat of 'Infowar' Brings CIA Warnings." Network World 13 September 1999. 25 April 2005 http://libproxy.nps.navy.mil/login?url=http://proquest.umi.com/pqdweb?did=44658533&Fmt=4&clientld=11969&RQT=309&VName=PQD.

Messmer, Ellen. "U.S. Army Kick-Starts Cyberwar Machine." CNN.com. 22 November 2000. 12 August 2005 http://archives.cnn.com/2000/TECH/computing/11/22/cyberwar.machine.idg/index.html.

"Middle East Cyberwar Could Spread to U.S." NewsMax.com 01 November 2000. 11 August 2005 http://www.newsmax.com/articles/archive/get2.pl?a=2000/10/31/202920

Page, Barnaby. "Pro-Palestinian Hackers Threaten AT&T." TechWeb.com 10 November 2000. 12 August 2005 http://www.techweb.com/wire/29116059

Pollitt, Mark M. "Cyberterrorism - Fact or Fancy?." Online posting. 2000. 27 August 2005. http://www.cs.georgetown.edu/~denning/infosec/pollitt.html.

Poulsen, Kevin. "CIA's 'Cyberwar' Is Just Computer Crime." ZDNet News 01 2001. 12 August 2005 http://news.zdnet.com/2100-9595_22-514749.html

Radcliff, Deborah. "Could a Cyberwar Cripple the U.S.?" CNN.com. 24 January 2001. 11 August 2005 http://archives.cnn.com/2001/TECH/computing/01/24/information.warfare.idg/index.html.

Rattray, Gregory J. Strategic Warfare in Cyberspace. Cambridge: The MIT Press, 2001.

Schwartz, John. "Hacker Defaces the American Israel Public Affairs Committee Pro-Israel Web Site: Intruders Grab E-mail Addresses and Credit Card Numbers." NY Times 03 November 2000. 03 November 2000 http://www.nytimes.com/2000/11/03/technology/03HACK.html

Schwartz, John. "When Point and Shoot Becomes Point and Click." The New York Times on the Web 12 November 2000. 12 August 2005 http://www.nytimes.com/2000/11/12/weekinreview/12SCHW.html

Shahar, Yael. "Information Warfare: The Perfect Terrorist Weapon." Online posting. 26 February 1997. ICT Internet Site. 24 May 2005. http://www.ict.org.il/articles/articledet.cfm?articleid=13.

Sobelman, Ariel T. "An Information Revolution in the Middle East?" Strategic Assessment June 1998. 26 May 2005 http://www.tau.ac.il.jcss/sa/v1n2p4_n.html.

Sobelman, Ariel T. "Is Everyone an Enemy in Cyberspace?" Strategic Assessment February 2000. 29 August 2005 http://www.tau.ac.il/jcss/sa/v2n4p4.html.

"Special Focus on Cyberwarfare." National Security. 2001. The Center for the Study of Technology and Society. 24 May 2005 http://www.tecsoc.org/natsec/focuscyberwar.htm.

Stein, George J. "Information War – Cyberwar – Netwar," in Battlefield of the Future: 21st Century Warfare Issues, http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html, last accessed on August 11, 2005.

Talbot, David. "Terror's Server: Fraud, Gruesome Propaganda, Terror Planning: the Net Enables It All. The Online Industry Can Help Fix It." Technology Review February 2005: Vol. 108, 46-51. Student Resource Center. Student Resource Center. Brandon High School Library, FL. 19 August 2005

Valeri, Lorenzo, and Michael Knights. "Affecting Trust: Terrorism, Internet and Offensive Information Warfare." Terrorism and Political Violence Spring 2000: 15-36.

Verton, Dan. "Cohen: Superpower Status Has a Downside." Federal Computer Week 28 August 2000. 12 August 2005 www.fcw.com

Verton, Daniel. "New Cyberterror Threatens AF." Feceral Computer Week 03 May 1999. 12 August 2005 www.fcw.com

Verton, Dan. "Superpower Status Risks Cyberattack." Feceral Computer Week 24 August 2000. 12 August 2005 www.fcw.com

Verton, Dan. "U.S. May Face Net-Based Holy War." Computer World 13 November 2000. 17 November 2000 http://www.computerworld.com/cwi/story/0,1199,NAV47-81_STO53940,00.html

Whine, Michael. "Cyberspace: A New Medium for Communication, Command and Control by Extremists." Online posting. April 1999. ICT. 27 August 2005. http://www.ict.org.il/articles/cyberspace.htm.

Wilson, Clay. "Information Warfare and Cyberwar: Capabilities and Related Policy Issues." CRS Report for Congress 19 July 2004. 23 May 2005 http://www.fas.org/irp/crs/RL31787.pdf.

Wrona, Jacqueline-Marie W. Appendix A in the Naval Postgraduate School Thesis entitled "From Sticks and Stones to Zeros and Ones: The Development of Computer Network Operations as an Element of Warfare – *A Study of the Palestinian-Israeli Cyberconflict and What the United States Can Learn from the 'Interfada'."* Naval Postgraduate School, September 2005.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Dan C. Boger, Ph.D.
   Naval Postgraduate School
   Monterey, California

4. LtCol Karl D. Pfeiffer, USAF, Ph.D.
   Naval Postgraduate School
   Monterey, California

5. Dr. James Forest, Ph.D.
   Director of Terrorism Studies
   Combating Terrorism Center
   United States Military Academy
   Lincoln Hall
   West Point, New York

6. ENS Jacqueline-Marie W. Wrona
   Valrico, Florida